



**SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO A  
VIVIENDAS**

**DAVID LEONARDO CASTAÑO SAAVEDRA  
JUAN DAVID ALONSO SIERRA**

**TRABAJO DE GRADO PARA OTORGAR EL TÍTULO DE INGENIERO  
ELECTRÓNICO Y DE TELECOMUNICACIONES**

**DIRECTOR  
JOSE ROBERTO CUARÁN VALENZUELA  
INGENIERO ELECTRÓNICO, MSC.**

**UNIVERSIDAD CATÓLICA DE COLOMBIA  
FACULTAD DE INGENIERÍA  
INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES  
BOGOTÁ  
2019**



**UNIVERSIDAD CATÓLICA**  
**de Colombia**

**SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO A  
VIVIENDAS**

**DAVID LEONARDO CASTAÑO SAAVEDRA  
JUAN DAVID ALONSO SIERRA**

**TRABAJO DE GRADO PARA OTORGAR EL TÍTULO DE INGENIERO  
ELECTRÓNICO Y DE TELECOMUNICACIONES**

**DIRECTOR  
JOSE ROBERTO CUARÁN VALENZUELA  
INGENIERO ELECTRÓNICO, MSC.**

**UNIVERSIDAD CATÓLICA DE COLOMBIA  
FACULTAD DE INGENIERÍA  
INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES  
BOGOTÁ  
2019**



## Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)

La presente obra está bajo una licencia:

**Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)**

Para leer el texto completo de la licencia, visita:

<http://creativecommons.org/licenses/by-nc/2.5/co/>

### Usted es libre de:



Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

### Bajo las condiciones siguientes:



**Atribución** — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).



**No Comercial** — No puede utilizar esta obra para fines comerciales.

Nota de aceptación:

---

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Bogotá, Mes de 2019

## **AGRADECIMIENTOS**

Siendo uno de los días más importantes de mi existencia, deseo dirigirme a las personas que han sido fundamentales para el alcance de este logro que a partir del momento marca mi vida, convirtiéndome en Ingeniero Electrónico y de Telecomunicaciones, sin dejar a un lado a la Universidad Católica de Colombia que con gran orgullo digo que es una de las instituciones más prestigiosas del país. Por otra parte, no puedo obviar al MSc José Curán, quien, con sus vastos conocimientos, dejó a un lado sus títulos para dedicarse a este grupo de jóvenes con ansias ávidas de conocimiento, convirtiéndose en nuestro guía y tutor con inmenso espíritu de humildad.

Así mismo lleno de orgullo y alegría, dedico y comparto mi título a quienes siempre han estado ahí a pesar de los avatares y de los altibajos, a pesar de las vicisitudes que se me han presentado, son los seres por los cuales el día a día se hace más emotivo y esas personas que han guiado e iluminado mi sendero, ellos son; mi señora Madre, mi señor Padre y mis dos hermanitos, les manifiesto mis más profundos sentimientos de admiración, lealtad, cariño y mucho más que eso, recordarles que los amo y mis éxitos desde luego dedicados a ellos. Gracias a mi Universidad, gracias a mis Maestros y gracias a mi hermosa Familia.

**David Castaño.**

Aprovecho la oportunidad que me brinda esta ocasión tan importante en mi vida para agradecer todo el apoyo y cariño recibido a lo largo de todos estos años vividos. Es en esta situación especial, cito especialmente al MSc José Roberto Cuarán, quien, como mi tutor del Proyecto Final de Carrera, fue de gran ayuda por su sabiduría y conocimiento, también he de agradecer tanto profesores como compañeros de clases y laboratorio, que aportaron su grano de arena y amistad para que hoy en día tuviese este gran reconocimiento, también a la Universidad Católica de Colombia que con su gran prestigio nos brindó este espacio para realizar tan bonita labor como la educación. Ahora y más importante aún, quisiera agradecer de todo corazón a mi familia quien siempre estuvieron hay en los momentos más difíciles de mi carrera y con esmero siempre me guiaron por el camino de la responsabilidad y honestidad, agradezco infinitamente a mi madre Isabel sierra, y a mi hermana Daniela Alonso quienes fueron mis pilares de felicidad y apoyo durante largas jornadas de trabajo, donde también y sin lugar a dudas me brindaron amor y comprensión durante toda la vida. Y por último quisiera agradecer a mi padre Humberto Alonso quien, aunque no esté presente con nosotros sé que desde algún lugar estará cuidando de mi familia y de mí, y hacerles saber a los tres que este proyecto y los demás éxitos en mi vida son dedicados directamente a ustedes tres por su gran amor y apoyo.

**Juan David Alonso Sierra.**

## TABLA DE CONTENIDO

1	INTRODUCCIÓN .....	16
2	ANTECEDENTES Y JUSTIFICACIÓN .....	18
2.1	ANTECEDENTES.....	18
2.2	JUSTIFICACIÓN .....	22
3	PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA.....	24
4	MARCO DE REFERENCIA .....	26
4.1	I.A. (INTELIGENCIA ARTIFICIAL).....	26
4.2	SISTEMA EXPERTO (SE).....	26
4.3	CÁMARA .....	28
4.3.1	Principio de funcionamiento de la cámara.....	28
4.3.2	Tipos de cámaras .....	30
4.3.3	Instalación de cámara para reconocimiento facial.....	30
4.4	PROCESAMIENTO DE IMÁGENES .....	32
4.5	PLACAS DE DESARROLLO .....	33
4.6	CONTROL DE ACCESO.....	33
4.7	TIPOS DE CONTROL DE ACCESO .....	34
4.7.1	Sistemas de control de acceso autónomos.....	35
4.7.2	Sistemas de control de acceso en red.....	35
4.8	MÉTODOS DE VERIFICACIÓN PARA EL CONTROL DE ACCESO.....	36
4.8.1	Verificación de dígitos. ....	36
4.8.2	RFiD. ....	37
4.8.3	Biometría. ....	38
4.8.4	Talanqueras o torniquetes.....	38
4.8.5	Reconocimiento ocular.....	39
4.8.6	Reconocimiento por huella dactilar.....	40
4.8.7	Reconocimiento facial. ....	41
4.9	FASES DE UN RECONOCIMIENTO FACIAL .....	42
4.9.1	Detección del rostro.....	43
4.9.2	Extracción de características.....	45

4.9.3 Reconocimiento.....	46
4.10 RECONOCIMIENTO DE IMÁGENES FIJAS.....	49
5 OBJETIVOS .....	51
5.1 OBJETIVO GENERAL.....	51
5.2 OBJETIVOS ESPECÍFICOS .....	51
6 ALCANCES Y LIMITACIONES .....	52
7 METODOLOGÍA.....	53
7.1 Fases del Proyecto.....	53
7.1.1 Etapa 1. Recopilación de información. ....	53
7.1.2 Etapa 2. Definición de requerimientos.....	54
7.1.3 Etapa 3. Selección de la técnica. ....	54
7.1.4 Etapa 4. Implementación del prototipo. ....	55
8. RECOPIACIÓN DE INFORMACIÓN .....	56
8.1 ANÁLISIS DEL COMPONENTE ESTADÍSTICO.....	56
8.1.1 Usuarios por sistema.....	56
8.1.2 Funcionamiento del sistema según el medio o factores externos. ....	58
8.1.3 Requerimientos. ....	61
8.2 ANÁLISIS DEL COMPONENTE FÍSICO.....	62
8.2.1 Tipos de placa de desarrollo .....	62
8.2.2 Características de las placas de desarrollo.....	67
8.2.3 Tipos y características de cámaras de reconocimiento facial.....	70
8.3 ANÁLISIS DEL ALGORITMO.....	74
8.3.1 Técnicas de reconocimiento facial. ....	74
8.3.2 Observación del comportamiento de las técnicas de reconocimiento facial.....	80
8.3.3 Bases de datos para el reconocimiento facial. ....	85
9. DEFINICIÓN DE REQUERIMIENTOS.....	87
9.1 REQUERIMIENTOS DE LA UNIDAD DE PROCESAMIENTO.....	87
9.2 REQUERIMIENTOS DE LA CÁMARA .....	88
9.2.1 Ergonomía.....	88
9.3 REQUERIMIENTOS DEL ALGORITMO .....	91

9.4 REQUERIMIENTOS DEL SOFTWARE.....	91
10. SELECCIÓN DE LAS HERRAMIENTAS DEL SISTEMA	10.1
HERRAMIENTAS HARDWARE .....	92
10.2 HERRAMIENTAS DE SOFTWARE.....	93
10.3 SELECCIÓN DE LA TÉCNICA DE RECONOCIMIENTO FACIAL .....	94
10.3.1 Eigen-Faces. ....	94
11. IMPLEMENTACIÓN DEL PROTOTIPO .....	99
11.1 ESQUEMA ELÉCTRICO .....	100
11.2 INSTALACIÓN DEL SOFTWARE .....	103
11.3 DETECCIÓN DEL ROSTRO Y CAPTURA.....	104
11.4 MANIPULACIÓN DE LA IMAGEN.....	108
11.5 EXTRACCIÓN DE CARACTERÍSTICAS Y ALGORITMO DE RECONOCIMIENTO .....	110
11.6 INTERFAZ GRÁFICA .....	112
11.6.1 Creación de la interfaz gráfica. ....	112
11.6.2 Guía de usuario de la interfaz. ....	115
11.7 PRUEBAS DE EFICACIA.....	118
11.7.1 Reconocimiento facial bajo características típicas de acceso. ....	125
12. RESULTADOS ESPERADOS.....	131
13. CONCLUSIONES.....	132
14. RECOMENDACIONES Y TRABAJOS FUTUROS.....	134
15. BIBLIOGRAFÍA .....	135



## LISTA DE FIGURAS

Figura 1. Pantalla de inicio del sistema de control. ....	19
Figura 2. Diagrama de comunicación entre plataformas. ....	20
Figura 3. Cara de una persona tratada por medio del método de Eigenface. ....	21
Figura 4. Estructura de un sistema experto. ....	27
Figura 5. Sistema de cámara de cine digital para grabación. ....	28
Figura 6. Diagrama de la realización del sistema de cámara de cine digital. ....	29
Figura 7. Ángulos, distancias y alturas de la posición de la cámara. ....	31
Figura 8. Diagrama de bloques de las etapas del procesamiento de imágenes. ...	32
Figura 9. Sistemas de control de acceso autónomo. ....	35
Figura 10. Sistemas de control de acceso en red. ....	36
Figura 11. Método de control de acceso por verificación de dígitos. ....	37
Figura 12. Método de control de acceso por RFID. ....	38
Figura 13. Método de control de acceso por Biometría. ....	38
Figura 14. Método de control de acceso torniquete. ....	39
Figura 15. Método de control de acceso por reconocimiento ocular. ....	40
Figura 16. Método de control de acceso por reconocimiento dactilar. ....	41
Figura 17. Método de control de acceso por reconocimiento facial. ....	42
Figura 18. Proceso del reconocimiento facial. ....	42
Figura 19. Algunas técnicas de detección facial. ....	43
Figura 20. Ejemplo de SVM. ....	48
Figura 21. Modelos de reconocimiento de patrones. ....	49
Figura 22. Estructura de la metodología. ....	53
Figura 23. Sobrexposición y sub-exposición de una imagen. ....	60
Figura 24. Arduino UNO. ....	62
Figura 25. Variedad de dispositivos Arduino y sus herramientas. ....	63
Figura 26. Raspberry Pi 3 B+. ....	64
Figura 27. Beaglebone. ....	65
Figura 28. Up square. ....	66
Figura 29. Intel Galileo Gen 2. ....	66

Figura 30. LaunchPad MSP-EXP430FR5969.....	67
Figura 31. Sensor Kinect. ....	71
Figura 32. Cámara V2 Raspberry Pi. ....	72
Figura 33. Cámara AXIS P1354.....	73
Figura 34. Cámara ECAM8000.....	74
Figura 35. Componentes principales de un conjunto de puntos bidimensional. ....	75
Figura 36. Ejemplo de reducción dimensional al aplicar PCA.....	76
Figura 37. Diferencia de PCA en LPP.....	77
Figura 38. Método de clasificación de Viola-Jones. ....	78
Figura 39. Esquema neuronal.....	79
Figura 40. Posición de la cámara.....	90
Figura 41. Diagrama de bloques de las señales independientes.....	96
Figura 42. Proceso de implementación del proyecto. ....	100
Figura 43. Diagrama de Raspberry pi 3 B+.....	101
Figura 44. Pantalla Táctil 3.5 pulgadas.....	102
Figura 45. Esquema de conexión del proyecto.....	102
Figura 46. Comandos para instalar OpenCV. ....	104
Figura 47. Comprobar la instalación de OpenCV.....	104
Figura 48. Archivo cascada. ....	105
Figura 49. Declaración de cámara.....	105
Figura 50. Cantidad de fotos tomadas por persona.....	105
Figura 51. Entrenamiento de modelo.....	106
Figura 52. Entrenamiento y programa finalizado. ....	106
Figura 53. Reconocimiento de rostro.....	107
Figura 54. Condicional si se desea entrenar el algoritmo o no. ....	107
Figura 55. Condicional si se desea entrenar el algoritmo o no. ....	108
Figura 56. Tratamiento de la imagen. ....	108
Figura 57. Captura vertical.....	108
Figura 58. Escala de grises. ....	109
Figura 59. Comando para ejecutar captura.py.....	109
Figura 60. Almacenamiento del nombre. ....	109
Figura 61. Función nombre.....	109
Figura 62. Primera parte de reconocimiento.....	110
Figura 63. Predicción.....	111
Figura 64. Segunda parte de reconocimiento.....	111
Figura 65. Librerías.....	112
Figura 66. Función principal de Interfaz.....	113
Figura 67. Función validar. ....	113
Figura 68. Función validar 2. ....	114
Figura 69. Función abrir ventana 2. ....	114
Figura 70. Función eliminar. ....	114

Figura 71. Función agregar/captura.....	115
Figura 72. Interfaz gráfica: Reconocimiento facial. ....	115
Figura 73. Interfaz gráfica: Clave de administración. ....	116
Figura 74. Interfaz gráfica: Clave de ingreso. ....	117
Figura 75. Interfaz gráfica: Administrador. ....	118
Figura 76. Reconocimiento facial de Checho (I). ....	119
Figura 77. Reconocimiento facial de Checho (II). ....	120
Figura 78. Reconocimiento facial de David (I). ....	120
Figura 79. Reconocimiento facial de David (II). ....	121
Figura 80. Reconocimiento facial de Mayra. ....	121
Figura 81. Reconocimiento facial de Juan. ....	122
Figura 82. Reconocimiento facial de David. ....	123
Figura 83. Activación de LED por medio de reconocimiento facial. ....	124
Figura 84. Prototipo final. ....	124
Figura 85. Pruebas David. ....	139
Figura 86. Pruebas Mayra. ....	140
Figura 87. Pruebas Checho. ....	141
Figura 88. Pruebas Juan. ....	142
Figura 89. Código de captura parte 1. ....	143
Figura 90. Código de captura parte 2. ....	144
Figura 91. Código de captura parte 3. ....	145
Figura 92. Código de reconocimiento parte 1. ....	146
Figura 93. Código de reconocimiento parte 2. ....	147
Figura 94. Código de reconocimiento parte 3. ....	148
Figura 95. Código de reconocimiento parte 4. ....	149
Figura 96. Código de reconocimiento parte 5. ....	150
Figura 97. Código de interfaz parte 1. ....	151
Figura 98. Código de interfaz parte 2. ....	152
Figura 99. Código de interfaz parte 3. ....	153

## LISTA DE TABLAS

Tabla 1. Parámetros de posición de la cámara.....	31
Tabla 2. Modelos de reconocimiento de patrones. ....	49
Tabla 3. Características principales de cada placa de desarrollo. ....	68
Tabla 4. Detalles de audio e imagen.....	68
Tabla 5. Redes y almacenamiento.....	69
Tabla 6. Software de la placa desarrolladora.....	70
Tabla 7. Exactitud de los algoritmos de reconocimiento facial frente a la variación de la pose. ....	80
Tabla 8. Resultados de los experimentos (12).....	80
Tabla 9. Comparación de las técnicas de reconocimiento facial basadas en EigenFace.....	81
Tabla 10. Comparación de los enfoques de reconocimiento facial basados en Gabor Wavelet.....	82
Tabla 11. Comparación de técnicas de clasificación en base a la red neuronal. ....	83
Tabla 12. Comparación de la identificación de las caras de una secuencia de video basada en el modelo oculto de Markov. ....	84
Tabla 13. Comparación de métodos de clasificación basados en SVM.....	85
Tabla 14. Resultados informados por diferentes grupos de investigación que prueban los tres algoritmos descritos. ....	97
Tabla 15. Ventajas de Eigenfaces y sus técnicas. ....	98
Tabla 16. Clasificación de porcentajes y tiempos para el reconocimiento facial. ....	125
Tabla 17. Pruebas de reconocimiento facial bajo condición lumínica. ....	125
Tabla 18. Clasificación de porcentajes y muestras para tabla de iluminación. ....	126
Tabla 19. Pruebas de reconocimiento facial bajo condición de accesorios. ....	126
Tabla 20. Clasificación de porcentajes y muestras para tabla de accesorios. ....	127
Tabla 21. Pruebas de reconocimiento facial bajo condición de ángulos de inclinación.....	127
Tabla 22. Clasificación de porcentajes y muestras para tabla de ángulos de inclinación.....	128
Tabla 23. Pruebas de reconocimiento facial bajo condición de gestos.....	128
Tabla 24. Clasificación de porcentajes y muestras para tabla de gestos.....	129
Tabla 25. Pruebas de reconocimiento facial bajo condición de características variantes. ....	130
Tabla 26. Clasificación de porcentajes y muestras para tabla características variantes. ....	130

## LISTA DE ANEXOS

ANEXO A.....	139
ANEXO B.....	143
ANEXO C.....	146
ANEXO D.....	151

## GLOSARIO

**CONTROL DE ACCESO:** Es el sistema que hace verificación de identidad de una persona para acceder a un lugar en específico.

**EIGEN-FACES:** Es una técnica de reconocimiento facial el cual se basa en un conjunto de vectores propios aplicados a la cara.

**RASPBERRY PI 3 B+:** Es una placa de desarrollo de bajo costo, la cual permite desarrollar proyectos informáticos, de forma educativa.

**RECONOCIMIENTO FACIAL:** Es una aplicación o método el cual permite reconocer o identificar automáticamente a una persona utilizando imágenes digitales del rostro o cuerpo.

**VISIÓN ARTIFICIAL:** Es una rama de la inteligencia artificial la cual se encarga de la manipulación de imágenes (adquirir, procesar, analizar y comprender) a través de un ordenador

## **RESUMEN**

Este trabajo de grado presentó el desarrollo de un sistema de reconocimiento facial el cual permitirá el control de acceso a una casa. Debido a la alta inseguridad que se evidencia en la ciudad, y los constantes robos en las viviendas, es imperativo crear alternativas que afronten este aspecto, ya que esta problemática afecta el estado de confort y seguridad en el hogar perjudicando en gran medida la salud de los ciudadanos sea física o mentalmente; por este hecho, se vio la necesidad de crear una solución que disminuya estos porcentajes de hurto utilizando un sistema de identificación biométrica facial, permitiendo que el acceso a nuestros hogares no depende de objetos que puedan perderse o caer en manos ajenas.

Durante el desarrollo del trabajo de grado se realizó la recopilación de información, análisis de requerimientos, tanto de un control de acceso como de los dispositivos que se utilizaron, y por último la implementación del control de acceso en el hogar y los aspectos a tener en cuenta para un funcionamiento ideal del sistema otorgando sus respectivas pruebas de funcionamiento y la eficacia del sistema al reconocer a una persona en diferentes expresiones faciales.

Con este sistema no solo se pretende brindar seguridad y confort al usuario si no incentivar el uso de herramientas tecnológicas como el reconocimiento facial, y dispositivos que están en el mercado, para implementar un control de acceso a viviendas seguro y de un bajo costo.

### **PALABRAS CLAVES:**

- Control de acceso.
- Visión artificial.
- Reconocimiento facial.

# 1 INTRODUCCIÓN

En la actualidad existen diversas tecnologías que ayudan a las personas a mejorar tanto calidad de vida, como tiempos y/o recursos en cierta tarea específica. Estas tecnologías se encuentran en entornos industriales e investigativos, pero muy poco se ve este desarrollo tecnológico dentro de un entorno de vivienda, el cual mejore sistemas presentes y brinden cierto tipo de confort y seguridad dentro del hogar. Para esto se aplican ciertas técnicas orientadas a automatización en una vivienda, que integran la tecnología en los sistemas de seguridad, bienestar y comunicaciones. Esto se conoce comúnmente como Domótica, la cual pretende realizar un ahorro energético y una mejor accesibilidad para el propietario.

Con el desarrollo tecnológico dentro del hogar se puede referir a aquellas aplicaciones y servicios que permiten mejorar la calidad de vida de los usuarios al aportar soluciones que facilitan la realización de tareas domésticas rutinarias, que suponen una comodidad añadida y que simultáneamente optimizan el consumo energético, seguridad y facilidad de uso.

Una de las características más relevantes de la automatización en el hogar es la seguridad, un factor bastante importante el cual brinda un tipo confort que incluye la satisfacción del usuario cuando entra y sale de su hogar, causando la sensación de seguridad al saber que sus puertas principales y demás objetos tecnológicos están dentro de un sistema seguro dado por el acceso al reconocimiento facial

En este proyecto, se lleva a cabo el diseño y la construcción de un sistema de seguridad con visión artificial, logrando dar un apoyo a la comodidad y al control versátil que el usuario tendría a la hora de entrar o salir de su hogar. De esta forma, cubre la necesidad de seguridad a través de un reconocimiento facial, el cual da la apertura a un control de puerta principal y activación o desactivación de una alarma, permitiendo un acceso mucho más personalizado del sistema para que el usuario pueda interactuar directamente con el control de sistema de seguridad.

De acuerdo a lo anterior, este proyecto condensó en 4 etapas la realización del sistema de reconocimiento facial de una forma muy clara y concisa, explicando en primera parte que tipos de tecnologías hay para un control de acceso, y los principios de uso del reconocimiento facial. En segundo lugar, para entender un poco más el aspecto donde se llevará a cabo el control de acceso, se investigaron algunos de los requerimientos que debe tener un control de acceso el cual implemente el uso de procesamiento de imágenes. En tercer lugar, se hace una selección de los aspectos y herramientas de hardware y de software ideales que cumplen cada uno de los requerimientos previstos, para poder implementarlo en el



hogar. Y, por último, se implementa el sistema teniendo en cuenta las pautas y requerimientos escogidos anteriormente para el uso y funcionamiento ideal, cabe aclarar que los dispositivos utilizados se encuentran en el mercado y las herramientas de software son Open source, algunos de estos objetos son la placa de desarrollo Raspberry Pi 3 modelo B +, una cámara full HD Ecam 8000 y una pantalla táctil de 3.5 pulgadas adherida a la placa de desarrollo, en cuanto al software se usó Linux distribución debían (Raspbian) para Raspberry pi, Python como lenguaje de programación junto con OpenCV para la manipulación de las imágenes.

## **2 ANTECEDENTES Y JUSTIFICACIÓN**

### **2.1 ANTECEDENTES**

En la Universidad de Antioquia, se presenta un artículo, donde se muestran características de tarjetas electrónicas llamadas ZigBee. También se presenta el diseño de estas tarjetas y de la interfaz de control, donde se determinan las tareas o las actividades a realizar. La aplicación de ZigBee se ve reflejada en la domótica, ya que brinda seguridad, confortabilidad y ahorro energético. El proceso de comunicación de estas tarjetas hacia la red eléctrica y posteriormente a la etapa de potencia, se puede realizar mediante microcontroladores, ya sea por comunicación serial o por señales inalámbricas, y esto es lo que permite el control de la vivienda por medio de la interfaz gráfica.<sup>1</sup>

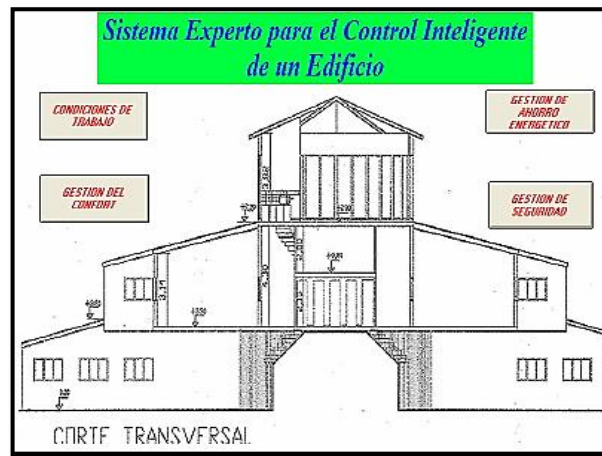
En Argentina se realizó un artículo que expone la cantidad de energía que se utiliza para sostener una edificación de gran tamaño, por eso llegan a la conclusión que la energía ambiental es la mejor sostenibilidad, para esto, se presentan sistemas inteligentes para modelar y controlar el comportamiento de los sistemas involucrados en la automatización de edificios, ya que esto permite optimizar considerablemente sus servicios prestados como la seguridad, el confort y el ahorro de energía, a continuación, en la figura 1 muestra las etapas necesarias del sistema experto, por medio de una interfaz gráfica, donde se evidencian los niveles para cada condición o gestión.<sup>2</sup>

---

<sup>1</sup> M. J. Barrera, N. Londoño, J. E. Carvajal and A. Fonseca, "Análisis y diseño de un prototipo de sistema domótico de bajo costo", Rev. Fac. Ing. Univ. Antioquia, no. 63, pp. 117-128, 2012.

<sup>2</sup> Sierra, E., Hossian, A., García-Martínez, R., & Marino, P. (2005). Sistema experto para control inteligente de las variables ambientales de un edificio energéticamente eficiente. Proceedings de la XI Reunión de Trabajo en Procesamiento de la Información y Control. Universidad Nacional del Comahueo. Pág. 446-452.

Figura 1. Pantalla de inicio del sistema de control.



Fuente: Sistema experto para control inteligente de las variables ambientales de un edificio energéticamente eficiente. Consultado: 18 de abril de 2019.

En la UNAM se presenta un estudio de la integración de técnicas de inteligencia artificial en ambiente domótico, donde garantiza la comodidad y seguridad para los usuarios dentro de su vivienda. Se implementa un controlador difuso para el aire acondicionado, control de ingreso por medio de reconocimiento facial y para el sistema de luces hay un servidor conectado que permite reconocer el clima y así manipular los sensores, actuadores y luces de la casa domótica. Por último, este sistema domótico, está conectado a servidores web, lo cual permite adaptarse al internet de las cosas.<sup>3</sup>

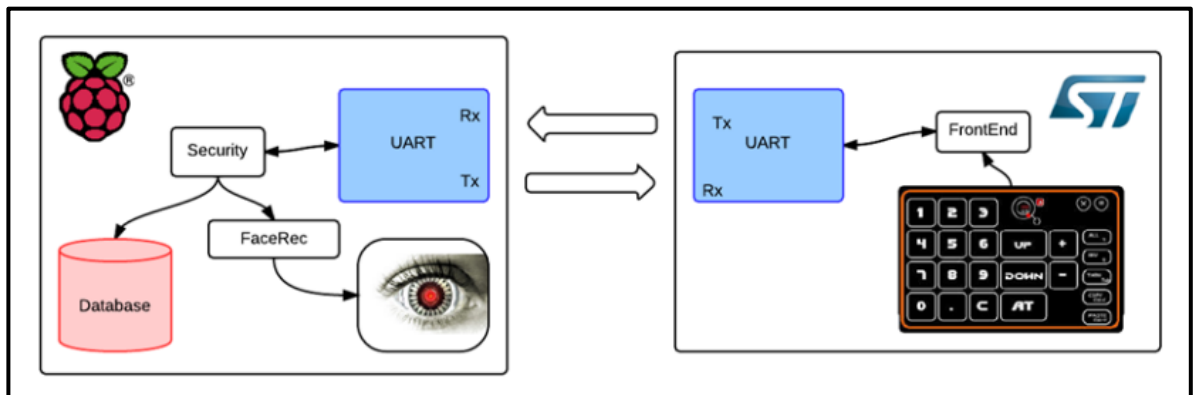
Se realiza la interacción de un actor virtual inteligente, este logra comunicación con el usuario, responde preguntas con respecto a la casa como luces, puertas, ventanas, entre otras. También confirma el estado de los electrodomésticos como cafeteras y televisores. El desarrollo de este actor virtual, consta de dos factores importantes; el primero son dos etapas necesarias para llegar al agente virtual; la primera etapa consta de un micrófono para que posteriormente pase a reconocer la voz, este cuenta con su propio identificador gramatical, la segunda etapa tiene un motor de búsqueda de respuestas con su propia base de datos, la tercera etapa contiene un sintetizador de voz para que este pase al segundo factor que es el

<sup>3</sup> Resendíz, G., Méndez, E., Sánchez, A. L., & Gudiño, F. (2017). Integración de técnicas de inteligencia artificial en ambiente domótico. Research in Computing Science, 135, 85-98

sistema Maxine, donde actúa como motor de generación, control de escenarios y caracteres virtuales.<sup>4</sup>

En la Universidad Complutense de Madrid, desarrollaron un sistema de seguridad basado en plataforma heterogénea distribuida, donde se despliega el sistema de seguridad que tiene por objetivo verificar y reconocer por medio de reconocimiento facial y contraseña a los usuarios que se encuentran registrados en una base de datos. En la parte izquierda de la figura 2, se evidencia la Raspberry Pi que es la placa encargada de procesar el algoritmo de reconocimiento facial y consultar la base de datos donde están almacenados los registros de los usuarios, y en la parte derecha, se observa el módulo de interfaz gráfica STM32F4 Discovery, que permite al usuario manipular el sistema por él mismo.<sup>5</sup>

Figura 2. Diagrama de comunicación entre plataformas.



Fuente: Sistema de Seguridad Basado en una Plataforma Heterogénea Distribuida.

Consultado: 04 de mayo de 2019.

En 2018, en la Universidad Politécnica Salesiana del Ecuador, desarrollaron un sistema de acceso usando tecnología RFiD y reconocimiento facial. Cuenta con un directorio donde se encuentran alrededor de 310 fotografías almacenadas y así poder realizar la comparación para luego arrojar el resultado de la verificación. Por otro lado, el hardware que se utiliza para este sistema es una Raspberry Pi 3 B+ y

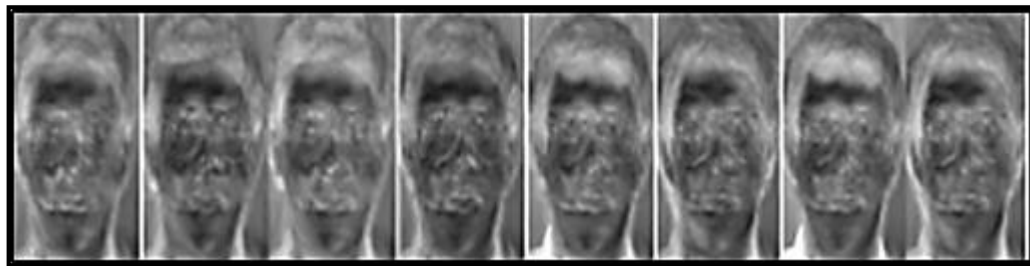
<sup>4</sup> Cerezo, E., Baldassarri, S., Cuartero, E., Serón, F., Montoro, G., Haya, P. A., & Alamán, X. (2007). Agentes virtuales 3D para el control de entornos inteligentes domóticos. In XIII Congreso Internacional de Interacción

<sup>5</sup> Lora, D.; et al. Sistema de Seguridad Basado en una Plataforma Heterogénea Distribuida. Enseñanza y Aprendizaje de Ingeniería de Computadores, 5: 29-38 (2015). [http://hdl.handle.net/10481/36567]

un lector de tarjetas de RFID, que es el encargado de enviar la información de la tarjeta a la Raspberry y así lograr el acceso de la persona.<sup>6</sup>

El departamento de ciencias de la computación de la Universidad de Alkharj KSA, lleva a cabo el reconocimiento facial por medio de entrevistas. Hay dos partes para la entrevista, en la primera se realiza una clase de preguntas sobre aspecto físicos como el envejecimiento, la oclusión parcial y las expresiones faciales, estas son almacenadas en bases de datos como AT & T, AR Database, FERET, ORL y Yale Database. En la segunda parte se trata de una entrevista más técnica, como lo es el reconocimiento por medio de métodos como Eigenface, Neural Network (NN), Support Vector Machine (SVM), Gabor Wavelet and Hidden Markov Model (HMM), ya que estos son análisis de datos por medio de vectores y valores de matriz de covarianza para analizar más a fondo la imagen captada por la cámara, como se demuestra en la figura 3. Estas entrevistas se realizaron con el fin de entrenar un algoritmo, y posteriormente, mejorar el rasgo de cada persona o personas y así obtener resultados mucho más óptimos al momento de realizar el reconocimiento facial.<sup>7</sup>

Figura 3. Cara de una persona tratada por medio del método de Eigenface.



Fuente: Face Recognition: A Survey. Consultado: 18 de mayo de 2019.

En noviembre de 2013, donde se expone que un sistema de seguridad puede ser controlado en cualquier parte del mundo, esto lo permite hacer ya que está conectado a internet, por otro lado, se ve la aplicación de IoT, y esto genera desarrollo tecnológico. Se utiliza una cámara inalámbrica, una campana y un sensor PIR, que son los dispositivos de entrada, mientras que los elementos de salida son; una pantalla LCD y la puerta electromagnética, estos dos últimos elementos, están

---

<sup>6</sup> Vega Luna, J. I., Sánchez-Rangel, F. J., Salgado-Guzmán, G., & Lagos-Acosta, M. (2018). Sistema de acceso usando una tarjeta RFID y verificación de rostro. Ingenius, (20), 108-118. doi:<http://dx.doi.org.ucatolica.basesdedatosezproxy.com/10.17163/ings.n20.201>

<sup>7</sup> Muhammad Sharif, Farah Naz, Mussarat Yasmin, Muhammad Alyas Shahid and Amjad Rehman. Face Recognition: A Survey. Department of Computer Science, Comsats Institute of Information technology WahCantt MIS Department CBA Salman bin Abdulaziz University Alkharj KSA.

conectados a la Raspberry Pi y esta está conectada a internet para tener una mejor experiencia y tendencia hacia internet de las cosas (IoT) por medio de la nube.<sup>8</sup>

En 2018, se implementa un sistema de seguridad para una vivienda. En el momento que la persona toca el timbre, automáticamente la cámara toma una captura de la cara de la persona que está esperando a que le abran, si la persona es conocida esta puede acceder a la casa sin ningún problema, si no, la captura de la persona desconocida se almacena en una base de datos, enviando un correo al propietario de la casa, permitiéndole enviar la confirmación de acceso a la persona nueva o negándole el acceso a esta.<sup>9</sup>

En el año 2009, se desarrolló un sistema automatizado de reconocimiento de expresión facial, utilizando técnicas de codificación como la AFFERS (Automated Facial Expression Recognition System), que procesan el video para luego arrojar el reconocimiento de las expresiones faciales y así obtener comparaciones más exactas con la base de datos y la persona que desea ingresar al sistema. Este sistema tiene un video procesamiento, que apunta hacia un modelado de formas y apariencias, para pasar a la clasificación de expresiones y por último irse al motor analítico que contiene informes, indicadores, tendencia de análisis y fotos instantáneas.<sup>10</sup>

## 2.2 JUSTIFICACIÓN

La cuarta revolución de la tecnología exige nuevas competencias en el desarrollo de sistemas inteligentes y automáticos tanto en la vida real como en la virtual, sobre todo con la aparición de nuevas tecnologías en el proceso de sistemas capaces de simular al ser humano.

A esto conviene agregar, que para facilitar algunos ámbitos de nuestra vida cotidiana se ha creado tal tecnología que no solo hace las tareas que le asignemos, sino, es capaz de razonar con su creador para mejorar la comunicación y optimizar estas tareas. Así mismo esta tecnología se ha utilizado un sinnúmero de veces para mejorar sistemas que ayuden a la calidad de vida y seguridad de las personas en la

---

<sup>8</sup> Md. Nasimuzzaman Chowdhury, Md. Shiblee Nooman, Srijon Sarker. Access Control of Door and Home Security by Raspberry Pi Through Internet. International Journal of Scientific & Engineering Research, Volume 4, Issue 11, November-2013 ISSN 2229-5518.

<sup>9</sup> P. B. Balla and K. T. Jadhao, "IoT Based Facial Recognition Security System," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, 2018, pp. 1-4. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8537344&isnumber=8537238>

<sup>10</sup> A. Ryan et al., "Automated Facial Expression Recognition System," 43rd Annual 2009 International Carnahan Conference on Security Technology, Zurich, 2009, pp. 172-177. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5335546&isnumber=5335506>

estadía del hogar, que en algunas ocasiones es perturbada por la inseguridad de la ciudad.

Por esta razón, la elaboración de este proyecto permitirá favorecer el estado de confort y seguridad de una persona integrando en un sistema de control de acceso para el hogar, un método inteligente como lo es la visión artificial, ya que es un proceso bastante eficiente para el reconocimiento de los propietarios, dado su bajo índice de error para disminuir la inseguridad de hurto en las viviendas de Bogotá, además de contribuir en el confort de sus ocupantes.

### 3 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

En Colombia el desarrollo tecnológico va en aumento dado que las empresas con procesos mecánicos avanzan para automatizar cada aspecto de ellas, desde la fabricación de algún objeto, el uso eficiente de energía, hasta la seguridad de la misma empresa. Esto hace que varios sectores se apropien de esta tecnología y quieran invertir en este aspecto de modernización ya que los beneficios son bastantes buenos para la industria y las grandes necesidades que esta cubre.

Por esta razón se ve mucho más frecuente el uso de inmótica la cual es el desarrollo de tecnología de automatización y control en un ámbito de inmueble (centros comerciales universidades y empresas) mientras que en la domótica maneja ambientes donde el desarrollo tecnológico es solo para hogares. Esta razón cumple varios objetivos donde interviene las aplicaciones donde se pueden generar el desarrollo, la infraestructura, la seguridad, tamaño y el costo.

Este desarrollo tecnológico ha sido tan satisfactorio que incluso se ha implementado en hogares, generando confort y seguridad, pero aún no está inmersa en la cultura ya que la mayoría de las personas no tiene el conocimiento de los beneficios que ofrece y desconocen su funcionamiento a la hora de suplir necesidades cotidianas. Además, cabe decir que por la complejidad de instalación y el costo de los mecanismos que requieren para la automatización del hogar es bastante compleja. Por esta misma razón personas de estratos bajos tienen cada vez menos posibilidades de obtener algunos de estos sistemas en su hogar.

Sin embargo, muchas personas en busca de cubrir la necesidad de control que brindan estos sistemas de seguridad y bienestar optan por comprar estos sistemas, que son poco eficientes y muchas veces inseguros. Además, las empresas que venden este tipo de sistemas de seguridad ofrecen sus servicios a unos costos bastante altos; así por ejemplo, según el periódico económico La Republica, “blindar una casa podría costar entre \$500.000 y más de \$30’000.000, de acuerdo con los sistemas físicos en inteligentes de seguridad que se desee instalar”<sup>11</sup>. Por esta razón, las personas buscan sistemas que brinden más seguridad al usuario sin que se vea afectado por el alto costo económico que conlleva la instalación y artefactos, además, de facilitar el uso para que el usuario pueda manejar el sistema.

No obstante, una de las características más relevantes que pueden otorgar estos sistemas es la seguridad en el hogar, dado que la inseguridad es uno de los problemas más recurrentes en la ciudad, y más aún los delitos contra el patrimonio

---

<sup>11</sup> MAYORGA Patarroyo Nicolás, 20 de mayo 2019 “Lo que le podría costar instalar sistemas de seguridad en su hogar” Columna La Republica, consultado el 16 de junio de 2019, disponible en: <https://www.larepublica.co/consumo/lo-que-le-podria-costar-instalar-sistemas-de-seguridad-en-su-hogar-2863423>



en los cuales se incluye hurto a personas, a establecimientos, vehículos, celulares y residencia. Este último es uno de los más preocupantes ya que se vulnera la seguridad e integridad de una persona dentro de su hogar donde se supone que es más seguro que en las calles. Según un balance de seguridad en Bogotá, más de 1630 denuncias de hurto en residencia se cometieron en el primer semestre del año 2017 en la ciudad, sin embargo “Durante el primer semestre de 2017, las denuncias de hurto a residencias se redujeron en un 21% con respecto al mismo periodo de 2016, con 430 casos menos. Febrero es el mes que presentó el menor número de casos en el semestre (210 casos).” esto quiere decir que, aunque haya una disminución con respecto al número de hurtos, este porcentaje sigue siendo muy alto.<sup>12</sup>

Por esta misma razón, se evidencia el crecimiento de la seguridad con técnicas avanzadas de tecnología. Según una publicación hecha por el espectador el pasado 3 de octubre del 2018 “la tecnología se convierte en un aliado para reducir la inseguridad en las ciudades. Un ejemplo evidente, impulsado desde las administraciones públicas, es el uso del Big Data y el internet de las cosas para prevenir los delitos y el vandalismo, conectando cámaras de seguridad con sistemas de analítica y video que permiten descifrar cuándo se requiere la intervención de la policía para prevenir un delito o para detener un delincuente.”<sup>13</sup>. Con esto, se concluye que la ciudad, en donde se evidencia un enorme problema con respecto a la seguridad requiere que sus ciudadanos cuenten con sistemas de seguridad donde se pueda entregar un control de acceso al usuario con un porcentaje muy alto en fiabilidad.

Las estadísticas anteriormente expuestas causan que la prioridad dentro de un sistema inteligente en un hogar sea la seguridad. Esta seguridad tiene bastantes servicios los cuales automatizan desde la entrada y salida de una persona en una vivienda hasta el control por medio de cámaras remotas que se encuentran unidas por medio de un dispositivo móvil, para un control de seguridad y confort

A raíz de esto se genera una pregunta. ¿Cómo implementar un sistema de control de acceso para viviendas basado en reconocimiento facial el cual sea confiable y de bajo costo?

---

<sup>12</sup> Díaz Mario, Maldonado Andrés Luengas, Balance de la seguridad de Bogotá No.53 , Cámara y comercio de Bogotá, pag 9, ISSN 2248-4906, Disponible en: <http://hdl.handle.net/11520/23187>

<sup>13</sup> Pardo Nicolás, 03 de octubre 2018 “La tecnología al beneficio de la seguridad ciudadana ” Columna el espectador, consultado el 3 de junio de 2019, pág. 1 disponible en: <https://www.elespectador.com/opinion/la-tecnologia-al-beneficio-de-la-seguridad-ciudadana-columna-816004>

## **4 MARCO DE REFERENCIA**

Dado que el proyecto de grado se centra en la implementación de un sistema de control de acceso a través de visión artificial, resulta fundamental dar definición a algunos conceptos básicos aplicables que están dirigidos hacia el proyecto.

En primera instancia se definen algunos conceptos básicos de un sistema de control de acceso, donde se podría aplicar este proyecto, además de exponer algunos conceptos que componen el ámbito de automatización en el hogar como la instrumentación necesaria dentro de ella.

### **4.1 I.A. (INTELIGENCIA ARTIFICIAL)**

Para Alan Turing la inteligencia artificial lo da como un ejemplo, en 1950 publicó un artículo llamado Computing machinery and intelligence, donde argumento en esta época que desde que una máquina de computación pueda actuar como un ser humano se le puede denominar un objeto inteligente. Este planteó un test donde se encierra a una persona en una habitación y a una máquina en otra donde no la puede ver el ser humano, si la persona no reconoce si es una máquina o un ser humano, en caso de ser una máquina se puede considerar inteligente, teniendo por referencia este test o prueba, el objeto que realice esta prueba y la apruebe, tiene las siguientes capacidades o características.<sup>14</sup>

- Aprendizaje.
- Representación de conocimiento.
- Razonamiento.
- Reconocimiento del lenguaje natural.

Por otro lado, la I.A. se puede ver en la robótica, en la visión artificial, entre otras grandes áreas de tecnología, por esta razón, hoy en día se habla que la inteligencia artificial, es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.

### **4.2 SISTEMA EXPERTO (SE)**

Un Sistema Experto es un sistema que emplea conocimiento humano capturado en una computadora para resolver problemas que normalmente requieran de expertos humanos. Un SE se caracteriza por.<sup>15</sup>

---

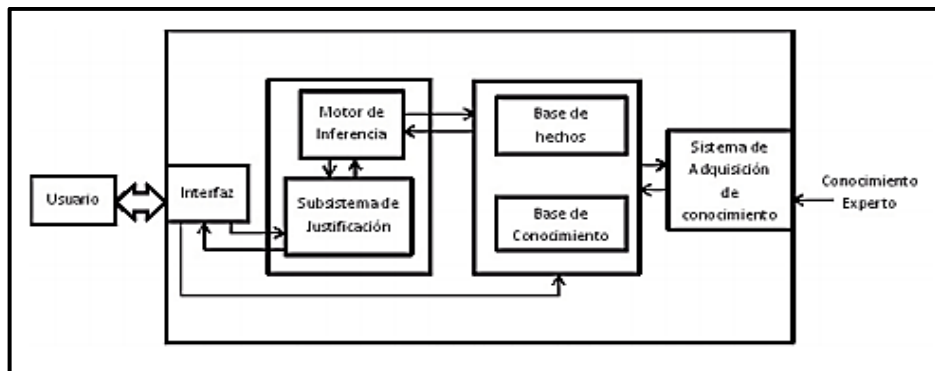
<sup>14</sup> GARCÍA, Alberto. Inteligencia Artificial. Fundamentos, práctica y aplicaciones. Rc Libros, 2012.

<sup>15</sup> BADARÓ, Sebastián; IBAÑEZ, Leonardo Javier; AGÜERO, Martín Jorge. Sistemas expertos: fundamentos, metodologías y aplicaciones. Ciencia y tecnología, 2013, no 13, p. 349-364.

- Estructura.
- Subsistema de adquisición de conocimiento.
- Base de conocimiento.
- Base de hechos.
- Motor de inferencia.
- Subsistema de justificación.

En la figura 4, Se muestra la estructura que conforma un Sistema experto, donde el conocimiento es ingresado por un experto en el área y se guarda en una base de datos, esta tiene dos funciones guardar nueva información del experto y guardar los hechos a los cuales el usuario está consultando. Este sistema se caracteriza por ser un método de retroalimentación donde el conocimiento se renueva dependiendo de la petición y la respuesta afirmativa o negativa del usuario en cuanto a una situación.

Figura 4. Estructura de un sistema experto.



Fuente. Estructura de un Sistema Experto. Tomado de: Sistemas Expertos: Fundamentos, Metodologías y Aplicaciones. Consultado: 3 de junio de 2019

Existen diversos tipos de sistemas expertos, donde cada uno tiene una especialidad dependiendo el área donde esté o el uso que se dé.

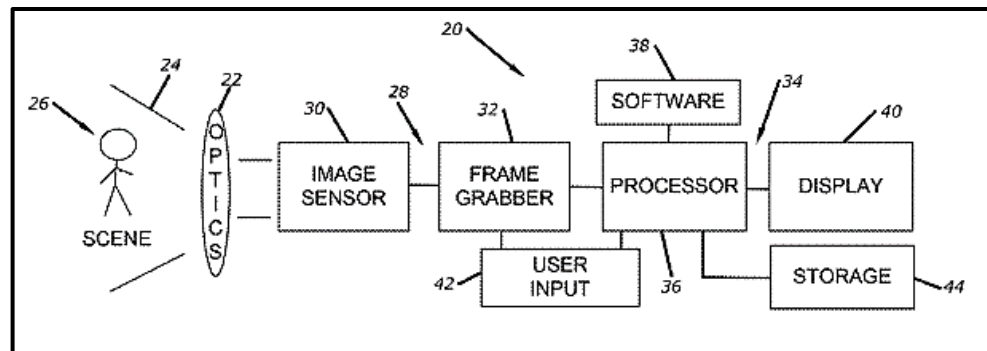
- Basados en reglas previamente establecidas.
- Representación del conocimiento.
- Reglas “Si...entonces...”.
- Basados en casos.

- Basados en redes bayesianas.
- Sistemas Expertos difusos.

### 4.3 CÁMARA

**4.3.1 Principio de funcionamiento de la cámara.** En la figura 5, se presenta el esquema de un sistema de cámara de cine digital para grabación, la cual se basa en el principio de las cámaras fotográficas.

Figura 5. Sistema de cámara de cine digital para grabación.



Fuente: Appearance-Based Statistical Methods for Face Recognition. Consultado: 19 de agosto de 2019

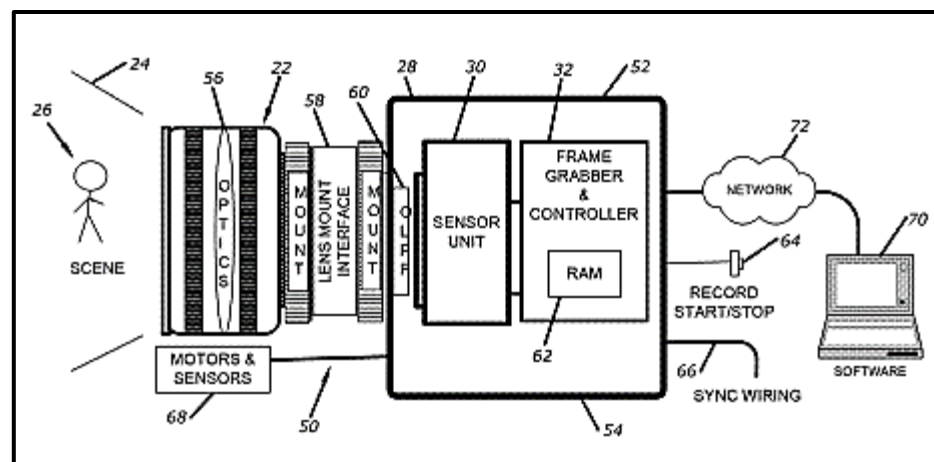
El sistema de cámara 20, incluye el conjunto óptico (22) para captar la luz de (24) cualquier tipo de escena (26) deseada, este sistema incluye un subsistema de imagen modular (28) alineado con el conjunto óptico (22), el subsistema comprende de uno o más generadores de imágenes, 30, donde incluye por lo menos un capturador de fotogramas (32), este generador de imágenes captura imágenes de alta definición a velocidades de película o video para HD, 2K y 4K, el generador lo compone; un sensor de imagen de pixel activo semiconductor de óxido de metal (CMOS), un sensor de imagen de pixel activo semiconductor de óxido de metal (MOS), un dispositivo de carga acoplada (CCD), un sensor de imagen de contacto (CIS), entre otros dispositivos de detección de pixeles y por último un único sensor de imagen que incluye filtros de color que se utilizan para la captura de imágenes a todo color.

El sistema 20 incluye una montura de lente que se interconecta el subsistema de imagen modular y el con el conjunto óptico (22) el cual lo compone el lente. La unidad de sensor de imagen 30, incluye unos mecanismos de ajuste los cuales

como su nombre lo indican ajustan la posición de la unidad del sensor de imagen con respecto al centro óptico de proyección del lente pero también sirve para ajustar la co-planaridad de una placa de detección (Superficie que sostiene la placa de circuito del sensor de imagen), en relación con el montaje de la interfaz óptica, también incluye un ajustador para el enfoque posterior, esta unidad, puede integrar un divisor de haz óptico o un mecanismo de obturador giratorio para permitir el uso de un visor óptico mientras captura y adquiere imágenes.

Por otro lado, la cámara de la figura 6, que se observa a continuación contiene varios componentes agregados, pero con el mismo principio ya descrito anteriormente<sup>16</sup>.

Figura 6. Diagrama de la realización del sistema de cámara de cine digital.



Fuente: Digital camera system for recording, editing and visualizing images.  
Consultado: 19 de agosto de 2019

<sup>16</sup> PRESLER, Ari M. Digital camera system for recording, editing and visualizing images. U.S. Patent No 9,565,419, 7 Feb. 2017.

### 4.3.2 Tipos de cámaras

**4.3.2.1 Cámara infrarroja.** Esta es perfecta para lugares oscuros y aplica para la vigilancia las 24 horas al día, de forma automática enciende el infrarrojo en el momento que hay menos luminosidad.

**4.3.2.2 Cámara de interiores.** Se trata de las cámaras caseras, estas no necesitan de grandes características en cuanto a la luminosidad (nocturnas, infrarrojas, etc.), ya que permanecen en lugares iluminados.

**4.3.2.3 Cámaras Antirrobo.** Este tipo de cámara por lo general está ubicado en zonas urbanas, por lo que debe tener una carcasa resistente a golpes, lluvia, calor, entre otros.

**4.3.2.4 Cámaras IP.** Estas se conectan directamente a internet para enviar o subir la información a la nube, así mismo se puede observar la imagen que esté transmitiendo mediante un dispositivo configurado con la cámara y conectado a internet.

**4.3.2.5 Cámaras con Movimiento y Zoom.** Se utilizan para circuitos cerrados de Tv (CCTV), donde existe una persona monitoreando la cámara y esta les realiza movimiento o zoom.

**4.3.2.6 Cámaras Ocultas.** También llamadas cámaras espías, por lo general se instalan dentro de algún objeto, como; detectores de humo, sensores de movimiento, espejos, tornillos, enchufes, entre otros, de esta forma no se ven y pasan por desapercibidas.

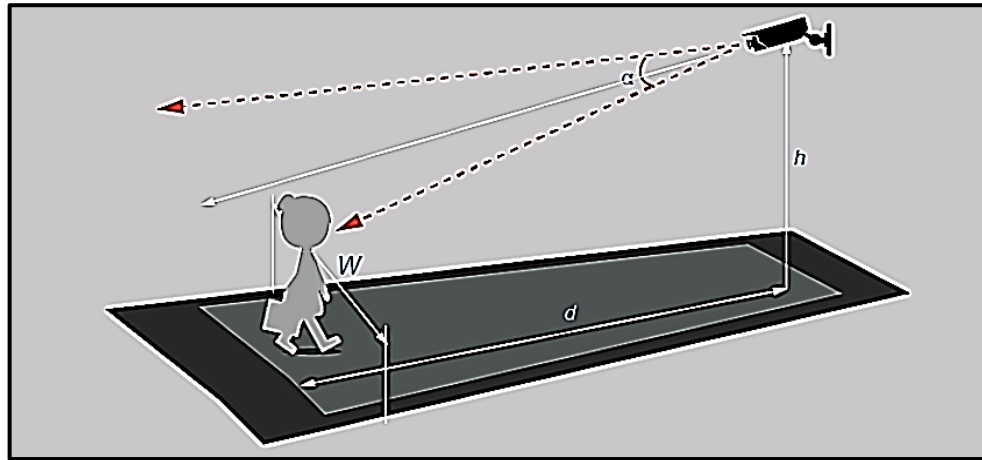
**4.3.3 Instalación de cámara para reconocimiento facial.** Al momento de instalar la cámara es muy importante tener en cuenta el ángulo de inclinación que debe tener esta, para poder visualizar desde una mejor perspectiva del rostro el cual se quiere reconocer, y por otro lado evita los objetos obstructores que puede haber dentro del recinto o del pasillo.<sup>17</sup>

La figura 7, se ilustra la correcta posición de una cámara de seguridad teniendo en cuenta la altura y el ángulo de instalación, y esto es para que el lente logre enfocar de una manera correcta la cara de las personas.

---

<sup>17</sup> Comunidad Huawei Enterprise. 2019. "El requisito de instalación para la cámara de reconocimiento facial" Pág 1. Disponible en: <https://forum.huawei.com/enterprise/es/el-requisito-de-instalaci%C3%B3n-para-la-c%C3%A1mara-de-reconocimiento-facial/thread/499177-100259>

Figura 7. Ángulos, distancias y alturas de la posición de la cámara.



Fuente: Comunidad Huawei Enterprise [www.huawei.com](http://www.huawei.com). Consultado: 23 de julio de 2019

- Los rostros a detectar pueden estar desviados a 15 grados hacia arriba o 30 grados hacia la izquierda o hacia la derecha.
- La altura recomendada para instalar la cámara está entre 2.5 metros a 3.5 metros.
- El ángulo de depresión recomendado de la cámara ( $\alpha$ ) es de 15 grados
- La distancia ( $d$ ) varía según la distancia focal del objetivo, se debe asegurar de que el foco de la lente de la cámara esté en la entrada o que exista un corredor.

Para una instalación adecuada se tiene que tener en cuenta también las características de la cámara como la longitud del foco, la distancia mínima y máxima de disparo, y la apertura del foco, por esto en la tabla 1 se evidencian estos parámetros de acuerdo a la altura de instalación de la cámara.

Tabla 1. Parámetros de posición de la cámara.

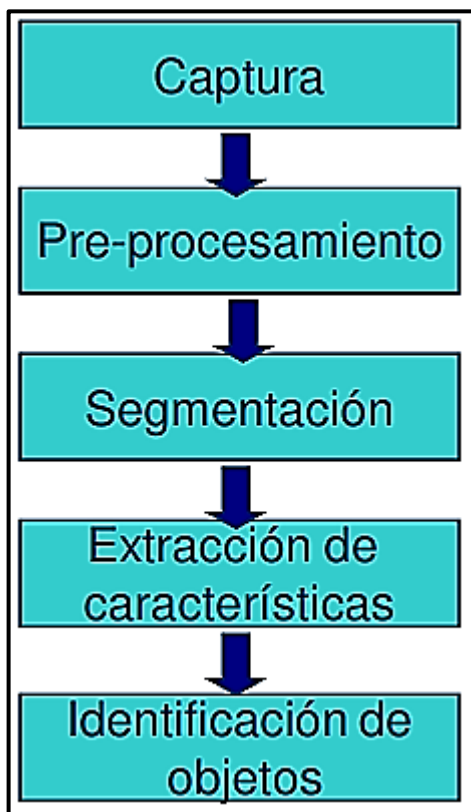
Longitud del foco (mm)	Distancia mínima de disparo (m)	Distancia máxima de disparo (m)	Ancho mínimo de vigilancia (m)	Ancho máximo de vigilancia (m)	Altura de instalación (m)
8	2	9	1	6	2.5 – 3.5
32	4	30	1	6	2.5 – 3.5
12	2	11	1	6	2.5 – 3.5
50	6	51	1	6	2.5 – 3.5

Fuente: Comunidad Huawei Enterprise [www.huawei.com](http://www.huawei.com). Consultado: 23 de julio de 2019

#### 4.4 PROCESAMIENTO DE IMÁGENES

Las imágenes tienen etapas de procesamiento las cuales se clasifican como se muestra en la figura 8, donde en primera instancia se hace la captura después pasa por un procesamiento para luego identificar los objetos capturados.<sup>18</sup>

Figura 8. Diagrama de bloques de las etapas del procesamiento de imágenes.



Fuente: Procesamiento digital de imágenes Pág. 4. Consultado: 14 de agosto de 2019

La primera etapa llamada captura, es donde la cámara capta el objeto, donde depende de distintas variables como lo es la distancia del objeto o persona, la resolución de la cámara (Mpx) y las propiedades que se aplican a la cámara para esta captura de imagen.

El pre-procesamiento, visualiza y procesa todo el entorno de la imagen que no es de interés como lo son las interferencias de otras personas, objetos, entre otros que no son de interés para el procesamiento de la imagen.

---

<sup>18</sup> Wainschenker, Rubén. 2011. "Procesamiento Digital de Imágenes Objetivos de La Materia." Pag 4-7. Disponible en: <http://www.exa.unicen.edu.ar/catedras/pdi/FILES/TE/CP1.pdf>



La segmentación, se encarga de fraccionar, reconocer y extraer las características, objetos o interferencias que tiene la imagen en el momento que se realiza la captura.

En la extracción de características como lo indica, es seleccionar las características que se desean para el procesamiento de la imagen, ya sea para un software o un algoritmo.

Al momento de identificar el objeto(s) o la persona de la que se quiere extraer las características, se debe analizar mediante un algoritmo que tenga características de decisión para que tome el camino correcto para seleccionar el objeto o la persona a procesar, para luego reconocerla, este algoritmo debe estar previamente definido.

#### **4.5 PLACAS DE DESARROLLO**

En general las placas de desarrollo son dispositivos compuestos por circuitos impresos que funciona mediante un microprocesador el cual posee una lógica específica sea cual sea el modelo la cual permite a desarrolladores, ingenieros y demás comunidad tener la capacidad de programar a un bajo nivel un dispositivo para el cualquier uso electrónico haciendo uso de entradas (Inputs) y salidas (Outputs). Son ampliamente utilizadas para la realización de proyectos emprendedores y de innovación debido a sus bajos costos y de fácil acceso.

Existe bastantes tipos de placas de desarrollo y entre ellas se distinguen algunas características que la hacen ideales para algunos proyectos, están diferencias parten de su potencial y función principal, algunas orientadas más a IoT (Internet de las cosas), otros para inteligencia artificial, y otras en poder de procesamiento etc.<sup>19</sup>

#### **4.6 CONTROL DE ACCESO.**

El control de acceso es un término muy usado en cuanto se refiere a la seguridad de un lugar o establecimiento, este es un componente muy importante ya que permite monitorear y controlar electrónicamente el tráfico de personas a través de objetos como puertas, ascensores, talanqueras, entradas principales etc.<sup>20</sup>

El control de acceso se encuentra en la mayoría de industrias y hogares donde se ve un tipo de automatización en el hogar y esto surge a través de la necesidad antigua de resguardar y proteger bien recursos u objetos o inclusive la propia seguridad del usuario. En base a esto se desarrolló una serie de soluciones basándose en la tecnología disponible en el mercado utilizando estándares y

---

<sup>19</sup> Lightpath. Tarjetas Para Desarrollo de hardware. [Consulta 9 de agosto, 2019], pág. 1 disponible en: <http://www.lightpath.io/tarjetas-de-desarrollo/>

<sup>20</sup> Seracis. Control de acceso. [Consulta 20 de mayo, 2019], pág. 1 disponible en <https://seracis.com/site/controles-de-acceso/>

arquitecturas abiertas lo cual posiciona como referencia dentro del sector de seguridad el control de acceso.

Algunas de las características más esenciales del control de acceso son:

- Restringir el paso a sitios por horarios, puertas y usuarios.
- Controlar flujo de personas por las instalaciones de una Compañía.
- Trazabilidad (Generación de Reportes).
- Registro de tiempos y asistencia.
- Control automático de entradas y salidas de vehículos o personas.
- Control de personas dentro de una edificación.
- Permite un control exacto del personal sin necesidad de presencia de supervisores para el registro de los ingresos y salida de los empleados.
- Protección de activos, reemplazo de llaves.
- Reemplazo de guardas y personal de seguridad.

#### **4.7 TIPOS DE CONTROL DE ACCESO**

Dado que los controles de acceso son sistemas automatizados que permite de forma eficaz, controlar el paso de personas a zonas restringidas en función de ciertos parámetros de seguridad establecidos por una empresa, establecimiento, comercio, institución o cualquier otro ente. Los controles de acceso también hacen posible llevar un registro automatizado de los movimientos de un individuo o varios dentro de un espacio determinado.<sup>21</sup>

Hay varias formas de clasificar los controles de acceso: sea por las dimensiones del espacio en el que se van a colocar o por la fuente de información que utilice el lector.

Con base a la primera opción, los controles se pueden dividir en:

1. Sistemas complejos: implican operaciones en red, destinados a grandes plantas industriales. Generalmente, requieren la apertura de varios controles de acceso o puertas.
2. Sistemas para establecimientos comerciales de mediana envergadura donde se suele necesita un control de acceso no tan robusto con la apertura de 2 a 4 puertas.
3. Sistemas pequeños destinados a locales de poco metraje o viviendas donde se requiera un control de acceso muy poco frecuente con la apertura de 1 o máximo 2 puertas.

---

<sup>21</sup> Sisca enseña, ¿Qué es un control de acceso? [Consulta 20 de mayo, 2019], pág. 1 disponible en: <http://sisca.co/que-es-un-control-de-acceso/>

**4.7.1 Sistemas de control de acceso autónomos.** Estos sistemas permiten controlar una o más puertas sin estar conectados a un ordenador o sistema central, quiere decir que este tipo de control de acceso no guarda registro de entradas o salidas.

Los controles de acceso autónomos más sencillos funcionan simplemente como una llave electrónica, es decir, solo identifican a la persona y le permiten ingresar o salir de las instalaciones.<sup>22</sup>

En la figura 9, se muestran algunos componentes necesarios para el sistema de control de acceso autónomos.

Figura 9. Sistemas de control de acceso autónomo.



Fuente: <https://images.app.goo.gl/zk68cFTYJzfqsJv8>. Consultado: 21 de mayo de 2019.

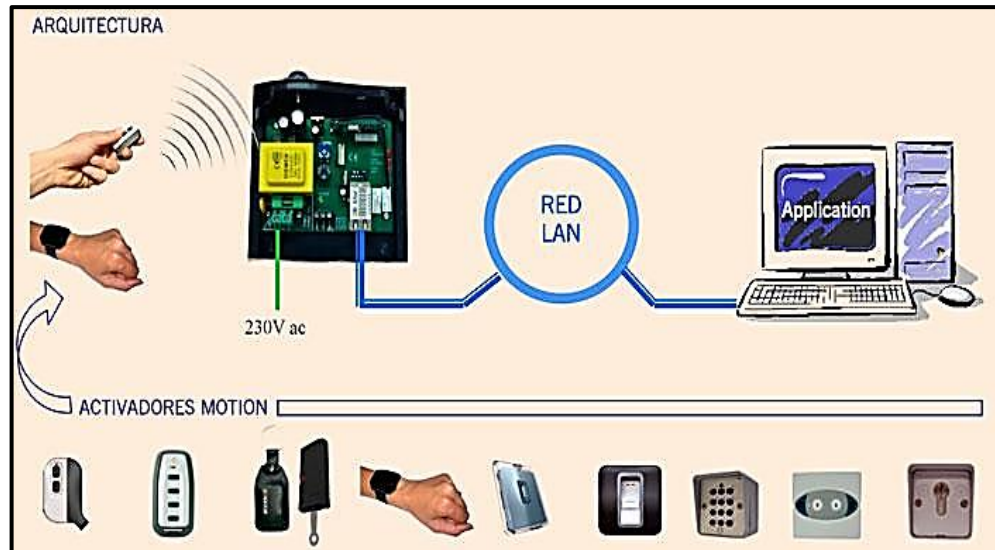
**4.7.2 Sistemas de control de acceso en red.** Estos sistemas son más complejos y cuentan con más funcionalidades que los anteriores, ya que se integran a través de un ordenador con un software que permite llevar el registro de todas las personas que entran o salen del centro, se puede extraer todo tipo de datos como la hora, fecha, también se ha utilizado en identificación, entre otros que se evidencian en la figura 10. Estos sistemas de control de acceso son totalmente personalizables para

---

<sup>22</sup> TD sistemas control y gestión, Qué es un sistema de control de acceso [Consulta 20 de mayo, 2019], pág. 1. disponible en: <https://www.tdsistemas.com/que-es-un-sistema-de-control-de-acceso/>

cada cliente, pudiéndose realizar combinaciones complejas que ofrecen funcionalidades adaptadas a cada necesidad.<sup>23</sup>

Figura 10. Sistemas de control de acceso en red.



Fuente: <https://images.app.goo.gl/DSqrfV2udXHTgvVG9>. Consultado: 21 de mayo de 2019.

## 4.8 MÉTODOS DE VERIFICACIÓN PARA EL CONTROL DE ACCESO

Para el control de acceso se utilizan un gran número de métodos para verificar que el usuario no es un impostor además de dar acceso al propietario de cualquier cosa que resguarde el control de seguridad, en el mercado existen grandes variedades de control de acceso desde los más complejos como lo son reconocimiento por biometría hasta una talanquera o control por verificación de dígitos.

**4.8.1 Verificación de dígitos.** Es un método tanto físico (figura 11) como digital, y se usa para el control de acceso a una cerradura, compuerta, caja fuerte etc. Estos métodos por verificación de dígitos son por lo regular dispositivos con teclado los cuales se ingresa un cierto número de caracteres los cuales verifican la entrada con una clave proporcionada por el usuario principal para a continuación dar acceso a una cerradura.

<sup>23</sup> TD sistemas control y gestión, Qué es un sistema de control de acceso [Consulta 20 de mayo, 2019], pág. 1, disponible en: <https://www.tdsistemas.com/que-es-un-sistema-de-control-de-acceso/>

Figura 11. Método de control de acceso por verificación de dígitos.



Fuente: <https://images.app.goo.gl/26g7bL7ymCmerXzj9>. Consultado: 3 de junio de 2019.

**4.8.2 RFiD.** Es un método automático de identificación el cual se basa en el almacenamiento y captura a distancia de datos usando dispositivos etiquetas o tags. Una etiqueta RFiD es un dispositivo pequeño como se muestra en la figura 12, que puede ser adherida o incorporada a un producto, o a una persona como una pegatina, con el propósito de identificarlo a distancia usando ondas de radio.

Los sistemas RFiD se componen básicamente de tres elementos:

**Tag RFiD:** Compuesto por una antena, un transductor de radio y un chip. Los hay de diferentes tipos, principalmente se clasifican en pasivas, activas y sema-activas.

**Lector RFiD:** Compuesto de antenas, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay algún tag en sus inmediaciones. Cuando capta una señal de un tag, extrae dicha información y se la pasa al sistema de procesamiento de datos.

**Sistema de procesamiento de datos:** Es una aplicación que gestiona y procesa los datos recibidos del lector RFiD <sup>24</sup>

---

<sup>24</sup> . Xiao, K., & Luo, L. (2013). A Novel Mobile Device NFC Stack Architecture. 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, 169–173. doi:10.1109/DASC.2013.57 19

Figura 12. Método de control de acceso por RfID.



Fuente: <https://images.app.goo.gl/YNRSg8rneq1eCGTV6>. Consultado: 3 de junio de 2019.

**4.8.3 Biometría.** Con la incorporación de estos conceptos a la tecnología se ha logrado prestar servicios de seguridad y fiabilidad para el ingreso de personal a instalaciones que así lo requieren. Un ejemplo de ello es el uso de lectores de huella dactilar en los controles de acceso.<sup>25</sup>

En la figura 13, se muestran en forma gráfica algunos de los métodos de Biometría tales como Face recognition (Reconocimiento facial), Voice recognition (Reconocimiento de voz), y el touch ID (reconocimiento dactilar)

Figura 13. Método de control de acceso por Biometría.



Fuente: <https://images.app.goo.gl/5w7XwHyoN7ccTqSd7>. Consultado: 3 de junio de 2019.

**4.8.4 Talanqueras o torniquetes.** Es un método de control de acceso el cual permite la entrada y salida de usuarios por medio de barras perpendiculares al armazón y que tiene una separación entre barra y barra el espacio necesario para

<sup>25</sup> Serratos, F. (n.d.). La biometría para la identificación de las personas, pág.14–16 disponible en: [https://www.academia.edu/31531606/La\\_biometr%C3%ADa\\_para\\_la\\_identificaci%C3%B3n\\_de\\_las\\_personas\\_Francesc\\_Serratos\\_PID\\_00195448](https://www.academia.edu/31531606/La_biometr%C3%ADa_para_la_identificaci%C3%B3n_de_las_personas_Francesc_Serratos_PID_00195448)

que pase una persona lo cual lo hace ideal para el control de acceso a personas identificando una por una, en la figura 14 se muestra el torniquete, este método es muy eficiente ya que se puede acoplar en un sinnúmero de métodos como RFID, verificación de huella dactilar o verificación de dígitos etc.

Figura 14. Método de control de acceso torniquete.



Fuente: <https://images.app.goo.gl/HaYvgwB6uGNSYuyj7>. Consultado: 3 de junio de 2019.

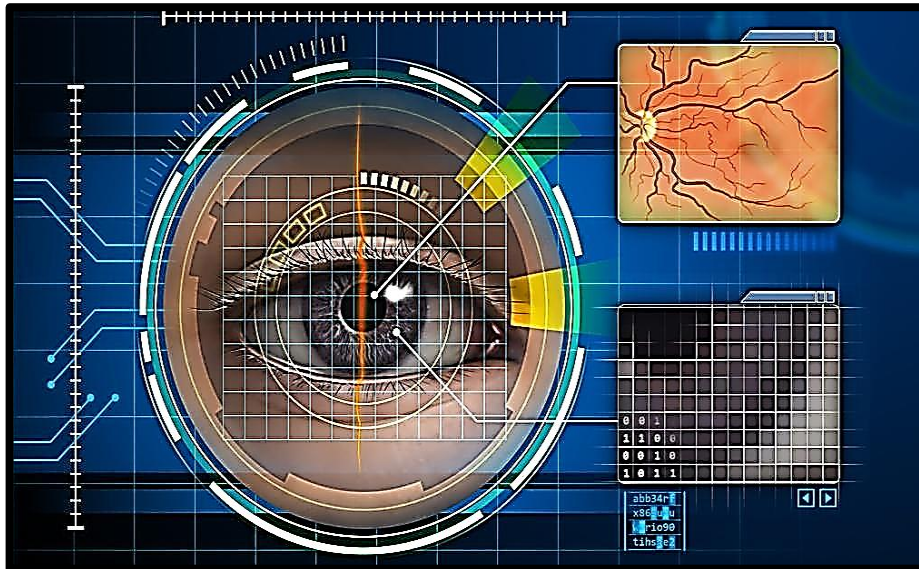
**4.8.5 Reconocimiento ocular.** Reconocimiento de iris/retina, es uno de los sistemas de identificación más usados ya que los patrones oculares cuentan con una probabilidad de coincidencia muy cercana a cero dados a que anteriormente se almacena una imagen en una base de datos para la comparación de los patrones oculares por lo tanto es un sistema demasiado eficiente dado que los ojos son el único órgano humano que a pesar de los años nunca envejece o cambia su aspecto físico. A pesar de esto posee algunas desventajas ya que al realizar la lectura con un láser es incómodo para el usuario y además si este usa lentes se verá afectado su patrona y no podrá realizarse la identificación, a continuación, en la figura 15 se evidencian algunas características del ojo humano <sup>26</sup>.

---

<sup>26</sup> Meneses alvaro, vargas cristian; diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco josé de caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar; universidad distrital francisco josé de caldas facultad de ingeniería ingeniería electrónica, pág 26. disponible en : <http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGerman2016.pdf>



Figura 15. Método de control de acceso por reconocimiento ocular.



Fuente: <https://images.app.goo.gl/YhejgYcn3EEc6MVt6>. Consultado: 3 de junio de 2019.

**4.8.6 Reconocimiento por huella dactilar.** La huella dactilar ha sido uno de los parámetros físicos para la caracterización de una persona, dada su buena eficacia para determinar la identidad de alguien ya que se ha comprobado que no existen huellas similares ni siquiera entre gemelos o entre dedos de la misma persona. El uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica. Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada. En este proyecto se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos, en la figura 16, se evidencia una huella dactilar.<sup>27</sup>

<sup>27</sup> Meneses alvaro, vargas cristian; diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco josé de caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar; universidad distrital francisco josé de caldas facultad de ingeniería ingeniería electrónica, pág 25. disponible en: <http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGerman2016.pdf>



Figura 16. Método de control de acceso por reconocimiento dactilar.



Fuente: <https://images.app.goo.gl/RVgRAzvQ9fvubYrX9>. Consultado: 3 de junio de 2019.

**4.8.7 Reconocimiento facial.** El reconocimiento facial es una tecnología que últimamente está siendo abarcada por varias áreas de la investigación como el análisis de imagen, extracción de características de archivos digitales etc. esto es debido a que este proceso tecnológico puede emular la capacidad del ser humano de reconocer personas siguiendo un patrón específico ubicado en nuestro cerebro, según la revista científica investigación y ciencia “los estudios de neuroimagen han revelado que varias regiones del tamaño de un guisante radicadas en el lóbulo temporal (la zona del cerebro situada bajo la sien) están especializadas en el reconocimiento de las caras.

Los neurocientíficos las llaman áreas faciales.”<sup>28</sup>, estas zonas toman ciertas características faciales de la persona a reconocer como el color de la piel, tamaño de ojos, nariz y características únicas de cada persona y todo esto es un actividad seminconsciente dado que en algunas ocasiones el cerebro hace este reconocimiento sin que la persona se percate, teniendo esto en cuenta esta tecnología quiere replicar esta función siguiendo una serie de pasos como detección facial, análisis de características , comparación con base de datos.

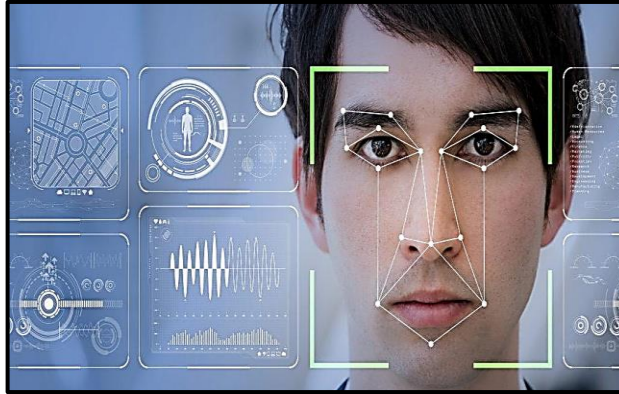
Por otra parte, se puede definir el sistema de reconocimiento facial como una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una fuente de

---

<sup>28</sup> Knvul Sheikh. 1 de agosto de 2017. Quedarse con la cara. INVESTIGACIÓN CIENTÍFICA, 711(15476), 5-6. Disponible en: <https://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/el-multiverso-cuntico-711/quedarse-con-la-cara-15476>

video, como se logra observar en la figura 17 y estas son comparadas con una base de datos.

Figura 17. Método de control de acceso por reconocimiento facial.



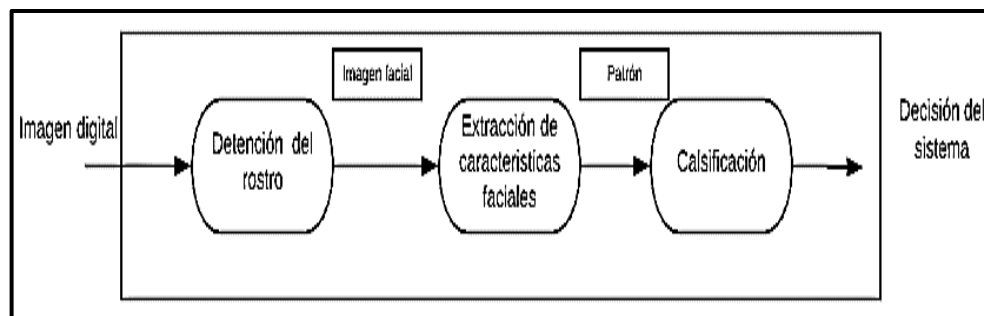
Fuente: <https://images.app.goo.gl/t5tsahKoF2NS2tRZA>. Consultado: 3 de junio de 2019

El reconocimiento facial es posible gracias a tres fases:

1. Detección del rostro.
2. Extracción de características.
3. Reconocimiento

En la figura 18, se muestra el proceso de reconocimiento facial, la cual sigue una línea donde la imagen pasa por varias fases para ser identificada.

Figura 18. Proceso del reconocimiento facial.



Fuente: Autores. Hecho: 9/07/2019

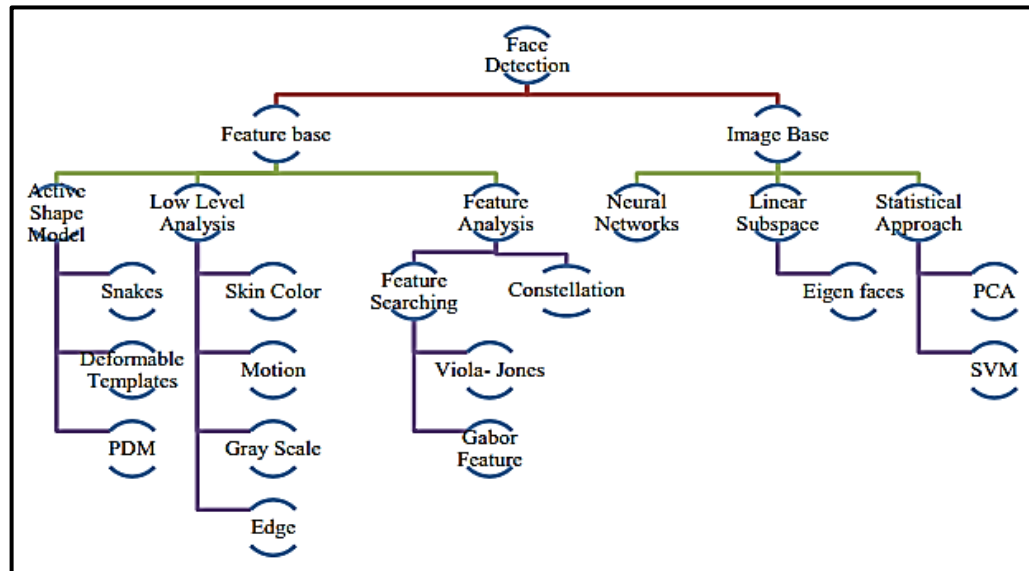
#### 4.9 FASES DE UN RECONOCIMIENTO FACIAL

En esta parte se van a manejar conceptos teóricos sobre el funcionamiento de los sistemas de control de acceso como el reconocimiento a partir de su proceso de detección facial, la extracción de características con los algoritmos que más

adelante se especificarán, por el último el reconocimiento que consiste en la clasificación de patrones extraídos del rostro.

Como primera parte se piensa seguir el orden del proceso de reconocimiento facial como se evidencia en la figura 18, por lo tanto, se describirán las fases para el reconocimiento facial apoyándose en el mapa conceptual de la figura 19.

Figura 19. Algunas técnicas de detección facial.



Fuente: Face Detection Approaches: A Survey. Consultado: 08 de julio de 2019.

**4.9.1 Detección del rostro.** La detección de un rostro se especifica como las áreas de una imagen digital donde se aprecia el rostro de una persona, esto implica que las áreas que no contienen rostro serán descartadas, o más bien, ignorar el fondo de tal manera que se haga una silueta del rostro identificado. Para la detección de rostro existen varios métodos que resuelven este problema como el uso de plantillas.

Como solo hay que detectar caras (sin identificar sujetos específicamente) se crean patrones para zonas que representan una cara y zonas que no; generalmente la solución para encontrar patrones que no son rostros, es por medio de la modalidad denominada “bootstrap”, o el método más conocido como EigenFace.

**4.9.1.1 Plantilla.** Esta es una técnica general empleada para detectar objetos de una escena, donde es representado por formas. Para la detección de una cara este debe tomar una característica del rostro como un ojo o una nariz y se utiliza una plantilla parametrizada que representa por medio de una función de energía los cual interpreta como valles y picos, luego esta plantilla interactúa con la imagen alterando algunos parámetros. Una vez ubicada la plantilla se ajustan sus parámetros para minimizar la función de energía.

**4.9.1.2 Bootstrap.** Esta técnica se basa en patrones que son rostros y se puede ver como clasificador, todos los falsos positivos se agregan como patrones de no-rostro y en una siguiente etapa, si aparecen nuevos falsos positivos, estos se siguen agregando como patrones.<sup>29</sup>

**4.9.1.3 AdaBoost.** Es un meta-algoritmo de aprendizaje automático basado en la idea de que contar con un grupo de expertos para tomar decisiones es mejor que tener uno solo. Al grupo de expertos se le conoce como ensamble y éste representa un clasificador fuerte, es decir, un clasificador con una precisión muy buena. Por su parte, a los expertos que conforman el ensamble se les denomina clasificadores débiles, es decir, clasificadores con una precisión menor. También es denominado un algoritmo adaptativo de machine learning cuyo nombre es una abreviatura de adaptative boosting.

Como segundo paso se habla del pre-procesado, esta depende de la información que se obtuvo en la detección. Esta etapa realiza una serie de transformaciones geométricas sobre la imagen dejándola preparada para la correcta extracción de característica y se utilizan cuatro fases para normalizar y alinear la imagen.

1. Rotación: Una de las utilidades de calcular las coordenadas de los ojos, radica en poder determinar el ángulo de giro de una cara en una imagen y compensarlo. Al tener caras sin giro, el proceso de reconocimiento dará mejores resultados.
2. Escalado: Para conseguir que todos los rostros de las imágenes tengan las mismas proporciones, se utiliza la distancia entre los centros de los ojos para conseguir un radio por el cual la imagen debe ser aumentada o reducida. Esto es necesario puesto que muchas técnicas de reconocimiento requieren que todos los datos de entrada tengan el mismo tamaño (en nuestro caso la matriz de píxeles).
3. Recorte: Una vez la imagen ha sido rotada y escalada, se procede al recorte de la misma para obtener sólo la región de interés. Se les da a todas las imágenes

---

<sup>29</sup> Scarel, German Matías. (2010). sistema de reconocimiento facial, Universidad Nacional del Litoral, Facultad de Ingeniería y Ciencias Hídricas, pág 16. Disponible en: [http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc\\_SMS10.pdf](http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc_SMS10.pdf)

las mismas dimensiones con el fin de que todas ellas tengan el mismo tamaño para que sea posible la comparación entre ellas.

4. Ecualización del histograma: Las imágenes pueden presentar variabilidad en la luminosidad y en el contraste lo que produce que imágenes similares sean muy diferentes respecto al valor de intensidad de sus píxeles. Mediante la ecualización de su histograma, se pretende que las imágenes que tienen la mayor parte de sus valores de intensidad concentrados en una zona reducida del histograma, pasen a extenderse por todo el rango de valores del histograma. Esto resulta en imágenes con mayor contraste y con menor variabilidad lumínica entre ellas.

**4.9.2 Extracción de características.** La extracción de características se refiere a la obtención de propiedades o parámetros particulares de cada rostro para luego poder ser clasificados, esto puede tomar tres enfoques diferentes.

- Enfoque holístico, basándose en la imagen del rostro como un todo.
- Enfoque mediante características locales, dando mayor importancia a las diferentes partes del rostro (geometría facial).
- Enfoque híbrido, basado en la idea de que el sistema de percepción humana combina características locales y globales para el reconocimiento.

Por otro lado, se pueden ver distintos métodos de extracción de características, parecidos a los enfoques anteriormente enumerados.

**4.9.2.1 Modelo de forma activa - Active Shape Model (ASM).** Esta característica se centra en rasgos complejos no rígidos, como lo es la apariencia física. El objetivo es localizar los puntos clave que tiene la cara, mediante un modelado estadístico en una imagen, como lo son; la nariz, boca, cejas, labios y ojos. El modelo estadístico facial se construye a partir de un conjunto de entrenamiento que contiene imágenes con puntos de referencia anotados manualmente. Los ASM se clasifican en tres grupos; Snakes, Deformable Templates y Point Distribution Model.<sup>30</sup>

- Snakes: Se utiliza para determinar los límites de la cabeza.
- Deformable Templates: Esta clasificación se generó para mejorar el rendimiento de Snakes, llevando la incorporación de información al ojo para mejorar la fiabilidad del proceso de extracción, por esta razón es necesaria esta clasificación.

---

<sup>30</sup> Modi, Mitul, and Fedrik Macwan. 2014. "Face Detection Approaches: A Survey." International Journal of Innovative Research in Science, Engineering and Technology 3 (4): 11107–16. Pag 11108. [www.ijirset.com](http://www.ijirset.com)

- Point Distribution Model (PDM): Este representa las formas faciales como vectores. Este modelo aprende constelaciones permitidas de dar forma a los puntos de los ejemplos de entrenamiento y usar componentes principales para construir lo que se llama una Point Distribution Model.

**4.9.2.2 Análisis de bajo nivel (Low Level Analysis).** Este se basa en características visuales de bajo nivel, como lo es el color de piel, movimiento, escala de grises y borde.<sup>31</sup>

- Skin Color: Es muy importante el color de piel para cada ser humano, a la misma vez es mucho más rápido el procesamiento de este que de otras características.
- Motion: El movimiento es muy importante, sobre todo cuando el uso de secuencia de video está disponible (grabando), ya que así se puede visualizar las siluetas como las partes de la cara y el resto del cuerpo.
- Gray Scale: Este puede ser muy importante ya que los rasgos faciales como cejas, pupilas y labios aparecen generalmente más oscuros que el resto de las regiones de la cara.

**4.9.3 Reconocimiento.** Esta etapa final está compuesta por dos ítems, los cuales hacen el trabajo de identificación de los patrones enviados por la etapa anterior y la verificación de estos patrones para una comparación de los patrones obtenidos con unos anteriormente establecidos por el sistema.

Este reconocimiento consiste en la clasificación de las características extraídas del rostro detectado, esta clasificación puede ser realizada de manera controlada, lo cual consiste en que un patrón de entrada es identificado como miembro de una clase ya predefinida. Sin embargo, hay una manera que no es controlada y esta es donde el patrón es asignado a una clase que no está predefinida o en otras palabras a una clase desconocida.

Para el reconocimiento, en cada clase hay un sujeto, por lo tanto, al clasificar las características extraídas de la cara del sujeto se está indicando a que sujeto pertenecen esos patrones, para el diseño de clasificadores se pueden distinguir tres aproximaciones basadas en:

1. Concepto de similitud.
2. Aproximación probabilística.
3. Optimización de un criterio de error.

---

<sup>31</sup> Modi, Mitul, and Fedrik Macwan. 2014. "Face Detection Approaches: A Survey." International Journal of Innovative Research in Science, Engineering and Technology 3 (4): 11107–16 Pag 11109. [www.ijirset.com](http://www.ijirset.com)

Como primera parte las aproximaciones basadas en concepto de similaridad son bastante breves ya que son simples e intuitivas, esto es porque los patrones similares son asignados a una misma clase y para esto se establece una métrica la cual define la similaridad para después clasificarla por medio una plantilla o mínima distancia usando uno o varios prototipos por clase

Un ejemplo de su efectividad es el uso de esta aproximación en la técnica de Eigenfaces original la cual aplica la regla del vecino más cercano, utilizando como métrica la distancia Euclides, donde cada prototipo es la media de los patrones de entrenamiento.

El enfoque probabilístico se utilizan conceptos de la teoría de la decisión estadística para establecer los bordes de decisión de las diferentes clases, y se asume que estas características que representan a un patrón tienen una función de densidad probabilística ajustada a la clase.

La tercera aproximación se basa en construir los bordes de decisión optimizando algún criterio de error. El objetivo es minimizar el error de clasificación entre la respuesta deseada y la salida del clasificador. Un ejemplo de este tipo de clasificadores son las redes neuronales las cuales pueden considerarse como sistemas distribuidos y paralelos que consisten de pequeñas unidades de procesamiento masivamente conectadas. Están conformadas por redes de grafos ponderados donde los nodos son las neuronas artificiales y los bordes (con pesos) son las conexiones entre las neuronas de entrada y salida de la red. Para lograr una clasificación adecuada son entrenadas con un algoritmo de entrenamiento a partir de un conjunto de datos.<sup>32</sup>

#### **4.9.3.1 Métodos de clasificación**

Máquinas de vector soporte (Support Vector Machines: SVM): Estas máquinas se usan como una herramienta útil en el campo del reconocimiento de patrones. La aplicación más sencilla de esta técnica es el problema de clasificación binaria esto quiere decir la definición de dos clases.

La idea profunda consiste en encontrar una hipótesis  $H$  que minimice la probabilidad de error empírico, en pocas palabras la probabilidad de que  $H$  tenga un error en un conjunto de prueba seleccionado aleatoriamente.

La clave del procedimiento consiste en establecer una correspondencia entre las muestras en el espacio de entradas y otro conjunto de vectores transformados en un espacio de dimensión mayor o igual el también llamado espacio de

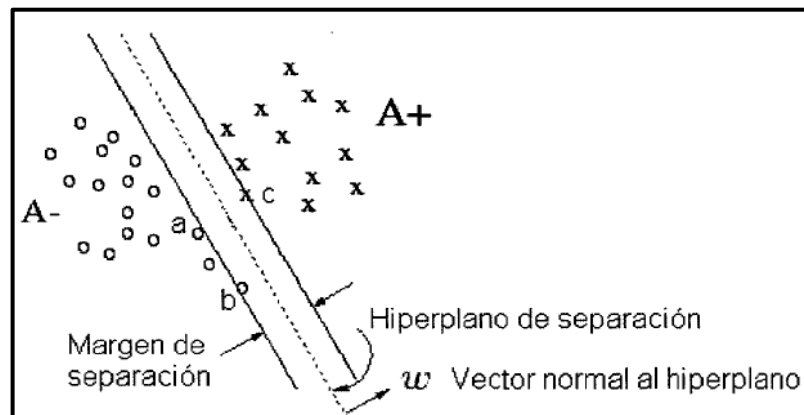
---

<sup>32</sup> Scarel, German Matías. (2010). sistema de reconocimiento facial, Universidad Nacional del Litoral, Facultad de Ingeniería y Ciencias Hídricas, pág 18. [http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc\\_SMS10.pdf](http://sinc.unl.edu.ar/sinc-publications/2010/SMS10/sinc_SMS10.pdf)

características. Para realizar este proceso se utiliza una correspondencia previamente definida como kernel. En el espacio de características se construye un hiperplano como se evidencia en la figura 20, esto equivale a minimizar el error empírico, este hiperplano óptimo separa las dos clases, por lo tanto, el procedimiento termina con una función de decisión lineal en el espacio de característica, donde los pesos se calculan como la solución de un problema cuadrático con restricciones.<sup>33</sup>

En la figura 20 se muestra el espacio entre los datos en diferentes dimensiones creando el hiperplano en SVM.

Figura 20. Ejemplo de SVM.



Fuente: Técnicas de reconocimiento facial mediante redes neuronales. Consultado: 30 de julio de 2019

K vecinos más próximos (K nearest neighbours, KNN): Las técnicas de clasificación basadas en esta técnica se encuentran en los planteamientos más clásicos de reconocimiento de patrones. Son rápidos y simples de usar.

Su principio de funcionamiento se basa en un conjunto dado de muestras de entrenamiento  $T_{ij}$  pertenecientes a una de las J clases diferentes  $C_1, \dots, C_j$ , un nuevo patrón desconocido X se asigna a la clase  $C_m$  que tenga un  $T_{im} \in C_m$  tal que sea la muestra del conjunto de entrenamiento más cercana a x de acuerdo con alguna métrica. En esta técnica se conoce como 1-NN, y en general estos métodos se consideran los k vecinos más cercanos de x dentro del conjunto de entrenamiento y se considera  $C_m$  como la clase que tiene más muestras entre los

<sup>33</sup> Cabello Pardos, Enrique. 2003. "Técnicas de Reconocimiento Facial Mediante Redes Neuronales," pág 30. Disponible en: <http://dialnet.unirioja.es/servlet/tesis?codigo=2586&info=resumen&idioma=SPA>.



k vecinos considerados. En la tabla 2, se muestra modelos de reconocimiento el cual plantea un enfoque, representación de píxeles y características.

Tabla 2. Modelos de reconocimiento de patrones.

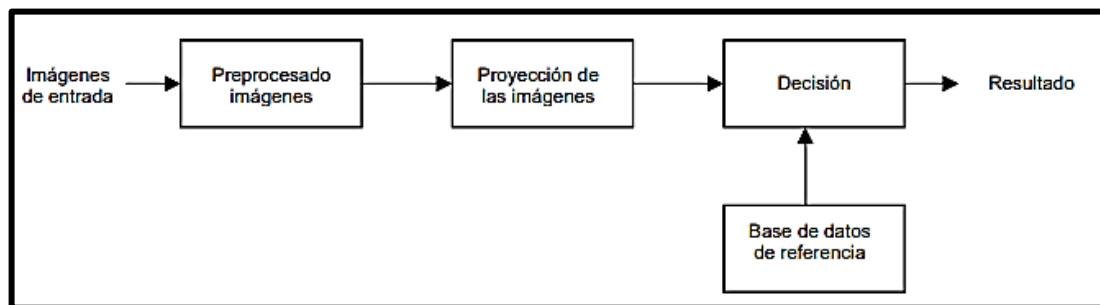
Enfoque	Representación	Función de reconocimiento	Criterio típico
Comparación de plantillas	Muestras, píxeles, curvas	Correlación, medida de distancia	Error de clasificación
Estadístico	Características	Función discriminante	Error de clasificación
Sintáctico o estructural	Primitivas	Reglas, gramática	Error de aceptación
Redes neuronales	Muestras, píxeles, características	Función de red	Error cuadrático medio

Fuente: Statistical Pattern Recognition: A Review. Consultado: 30 de julio de 2019

#### 4.10 RECONOCIMIENTO DE IMÁGENES FIJAS

El reconocimiento de imágenes fijas requiere una serie de pasos indispensables para su funcionamiento, estos pasos se especificarán en los bloques de la figura 21 donde más adelante se explicará cada uno de ellos.

Figura 21. Modelos de reconocimiento de patrones.



Fuente: Estudio de técnicas de reconocimiento facial. Consultado: 19 de agosto de 2019

El reconocimiento de imágenes fijas como su nombre lo dice, es un tipo de reconocimiento de que utiliza imágenes de referencia las cuales son almacenadas y conocidas por el sistema y son utilizadas para saber si una imagen de entrada o imagen test pertenece a un conjunto de imágenes anteriormente registradas.

Las imágenes test son las que se reciben en el sistema y se tienen que reconocer para su verificación. Dentro de estas imágenes hay unas llamadas imágenes de entrenamiento que son utilizadas para que métodos de reconocimiento como el PCA y LPP logren conseguir matrices de proyección que son los culpables del proceso de comparación de una imagen test con una imagen de referencia.

Como primera media, se ingresa una imagen que quiere verificarse y así dar un resultado positivo o negativo en similitud, para esto la imagen de entrada llega a un procesamiento donde la imagen es digitalizada y descompuesta por valores numéricos para que la máquina pueda entender la información que entra al sistema,

Ahora el set de imágenes de referencia y la imagen de test son procesadas y proyectadas para su debida comparación y para su reconocimiento se tiene que dar unas condiciones muy específicas dados por el sistema o método de reconocimiento facial o en tal caso su recuperación, se denomina de esta forma porque al realizar un proceso de verificación si la imagen corresponde a cierta similitud de una imagen en la base de datos, esta indicara su recuperación de la misma.

Cabe decir que el procesamiento y proyección de cada imagen difieren con el uso de diferentes técnicas de reconocimiento de imágenes.

## **5 OBJETIVOS**

### **5.1 OBJETIVO GENERAL**

Desarrollar un sistema de reconocimiento facial para el control de acceso de una vivienda.

### **5.2 OBJETIVOS ESPECÍFICOS**

- Recopilar información sobre técnicas de reconocimiento facial y la instrumentación necesaria.
- Definir los requerimientos de diseño del sistema de reconocimiento con base en las condiciones típicas de acceso a una vivienda.
- Seleccionar la técnica de reconocimiento facial que permita tener en cuenta las condiciones previamente definidas.
- Implementar un prototipo de prueba con el algoritmo de reconocimiento facial como medio de validación del diseño.

## 6 ALCANCES Y LIMITACIONES

Se desarrolló el sistema de reconocimiento facial, más no el mecanismo de acceso a la vivienda y se implementó en un software libre el cual sea compatible con la placa ordenador que se elija.

El desarrollo del sistema el cual contiene el algoritmo de reconocimiento facial sobre una placa de desarrollo debe cumplir las funciones como ordenador, y operar una cámara digital la cual identifique a un usuario. Dentro del sistema se implementó una base de datos para guardar los usuarios a los cuales dispone el algoritmo para hacer el reconocimiento.

Se desarrolló además una interfaz cómoda para el usuario principal donde pueda hacer gestión de los usuarios que tengan acceso al sistema como a los usuarios que debe reconocer el algoritmo para permitir su acceso a la vivienda.

El sistema llevará a cabo el reconocimiento en las condiciones típicas de acceso a una vivienda como, por ejemplo: acceso a la vivienda en diferentes franjas horarias; acceso de personas de diferente estatura. Durante el desarrollo del proyecto se identificarán otras condiciones típicas de acceso a viviendas.

La limitación de la condición típica de acceso es el contraluz generado por la luz natural por lo tanto se debe disponer de una cámara de alta definición con WDR.

El sistema de seguridad que contiene el algoritmo de reconocimiento facial, base de datos, interfaz de usuario, se desarrollará y probará en las instalaciones de la Universidad Católica simulando las condiciones de acceso a una vivienda por medio de un prototipo.

Cabe aclarar que el rápido reconocimiento, junto con el análisis y extracción de las características de cada persona dependerá de la capacidad y eficiencia tanto de la memoria RAM, y la velocidad de procesamiento del dispositivo escogido.

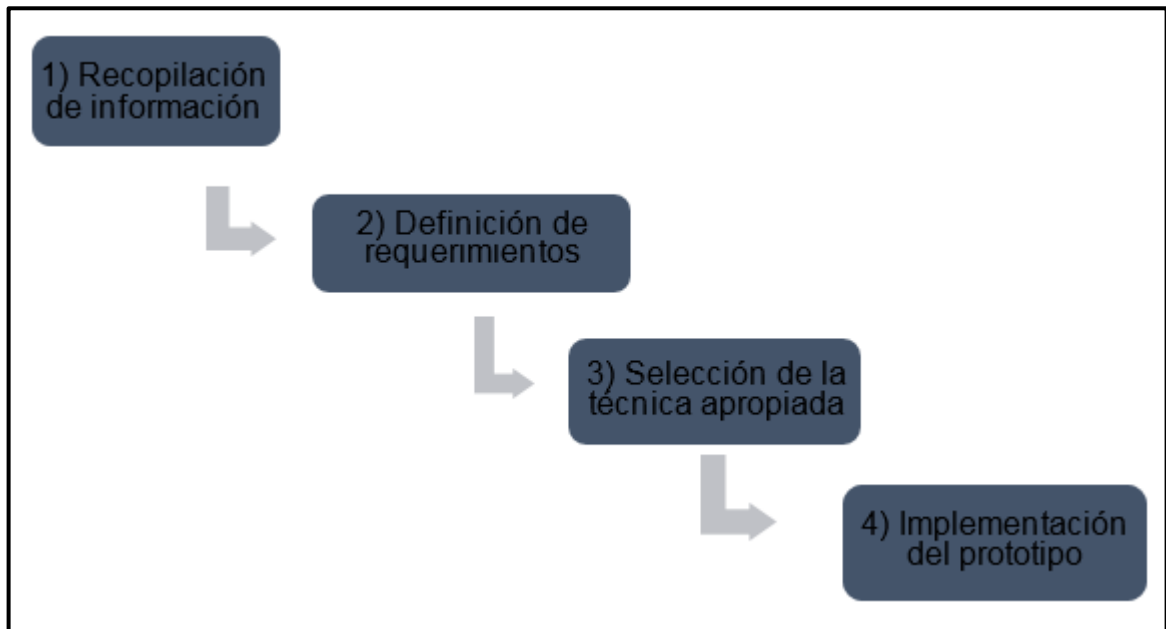
El sistema de reconocimiento tiene como facultad de reconocer mínimo 4 personas.

## 7 METODOLOGÍA

### 7.1 FASES DEL PROYECTO

A continuación, se describen las diferentes fases para el desarrollo del proyecto. Con base en los objetivos específicos, se siguen unas actividades cronológicamente. En la figura 22, se observa el orden para cada etapa.

Figura 22. Estructura de la metodología.



Fuente: Autores. Hecho: 2/05/2019

#### 7.1.1 Etapa 1. Recopilación de información.

Actividad 1.1. Se recopila información sobre técnicas de reconocimiento facial. Para esto se realiza una investigación avanzada en bases de datos con respecto a trabajos ya realizados y sus aplicaciones.

Además, se hizo un estudio de los mecanismos de control del acceso en la vivienda donde se tuvieron en cuenta.

- Mecanismos.
- Fiabilidad
- Porcentaje de error.
- confort.
- Costos.

Actividad 1.2. Se hizo un estudio previo del software ideal para la implementación del reconocimiento facial en un dispositivo. Para esto se realizaron comparaciones con softwares disponibles en el mercado los cuales en primera parte deben ser de libre acceso (Open source) y segundo, el más eficiente con la herramienta hardware que se utilice.

Además, se realizó el estudio y comparación de algunas placas de desarrollo para identificar la compatibilidad de estas con el software. Asimismo, cumplir con ciertas características como ser de bajo costo, ser compatible con una cámara digital para el respectivo análisis de imagen y tener un nivel de procesamiento alto.

### **7.1.2 Etapa 2. Definición de requerimientos**

Actividad 2.1. Se definió los requerimientos de diseño necesarios para la adaptación del control de acceso en la vivienda como:

- Acceso a la vivienda tras identificación del propietario.
- Especificación de nuevos propietarios para que accedan al sistema del control de acceso (Mínimo 4 personas).

Actividad 2.2. Se identificó las condiciones típicas del acceso al sistema donde se tuvo en cuenta varios aspectos como:

- Validar el acceso al reconocer al propietario.
- Impedir acceso si el sistema no reconoce a la persona.
- Interfaz para registrar, modificar, eliminar, y buscar usuarios que tengan acceso al sistema.
- Identificar condiciones de acceso típicas y de entorno controlado
- La influencia de aspectos climáticos.

Actividad 2.3. Se seleccionó la instrumentación requerida por el sistema de reconocimiento facial, así como también las herramientas de software necesarias.

### **7.1.3 Etapa 3. Selección de la técnica.**

Actividad 3.1. Se hizo una comparación de algunos algoritmos capaces de tomar fotos al usuario y tomar aspectos de ella para compararlas con la base de datos del propietario.

Actividad 3.2. Se realizó una extracción de características de cada técnica utilizada para el reconocimiento de imágenes faciales.

Actividad 3.3. Se escogió la técnica que está más acorde a las condiciones típicas que requiere el sistema y se hizo una profundización teórica de la técnica seleccionada.

#### **7.1.4 Etapa 4. Implementación del prototipo.**

Actividad 4.1. Se llevó a cabo la interconexión física entre los sensores (cámara), la unidad de control y la interfaz de usuario.

Actividad 4.2. Se realizó la programación de la unidad de control con un algoritmo de reconocimiento facial y la interfaz de usuario.

Actividad 4.3. Se hizo pruebas de eficiencia del sistema de reconocimiento facial bajo diferentes condiciones de acceso a una vivienda.

## 8. RECOPIACIÓN DE INFORMACIÓN

De acuerdo con la metodología, en esta parte se hizo una profundización de la información requerida por el sistema de reconocimiento facial para el control de acceso de una vivienda, lo cual comprende tres vertientes bastante importantes como lo son el componente estadístico, complemento físico, y por último el estudio del algoritmo.

El componente estadístico comprende el estudio de los requerimientos del sistema y condiciones típicas de acceso a la vivienda, además de los usuarios que debe haber por sistema.

- Usuarios por sistema.
- Funcionamiento del sistema según el medio o factores externos.
- Requerimientos: funcionales y no funcionales.

El componente físico se encargó de recopilar información sobre tipo de cámaras utilizadas para el conocimiento facial, además de eso, se realizó un estudio de las placas de desarrollo que hay en el mercado y cual tiene las mejores condiciones de funcionamiento para el proyecto.

El estudio del algoritmo comprendió las técnicas que se utilizan para el reconocimiento facial, debido a que este apartado contiene las características de algunos tipos de reconocimiento facial que hay en la actualidad, con sus respectivas eficiencias y capacidades, además de los algoritmos que se utilizan para el análisis digital de las imágenes tomadas por la cámara.

Para lograr esta actividad se planteó de forma ordenada una serie de pasos que condensan este proyecto, y logre una definición más clara de los parámetros, condiciones y requerimientos principales adecuadas para el funcionamiento de este proyecto de grado.

### 8.1 ANÁLISIS DEL COMPONENTE ESTADÍSTICO

Los requerimientos del sistema son esenciales al momento parametrizar el funcionamiento del sistema y ver el comportamiento ideal del proyecto. Para esto se tienen en cuenta las siguientes condiciones.

**8.1.1 Usuarios por sistema.** Los usuarios son una parte fundamental del sistema ya que estos son los que hacen uso del reconocimiento facial para un control de acceso en el hogar, por este motivo es necesario de cierto modo contar con algunas restricciones, y recomendaciones las cuales otorguen un mejor manejo del sistema,



además de esto poder brindar más seguridad y calidad a la hora de hacer el reconocimiento facial. Para que una persona se vuelva usuario del sistema tiene que estar registrado y con ello tener una serie de fotos para que el sistema en su defecto extraiga las características y reconozca estas fotos o imágenes.

Estas son llamadas imágenes de referencia, y se almacenan en una base de datos, y para que el sistema haga una comparación tiene que tener una foto o imagen de entrada la cual es llamada imagen de prueba. Para cada usuario se tendrá en cuenta una base de datos.

Esta base de datos agrupará las fotos de un solo usuario para que el sistema no correlacione la información con otro usuario. Para este grupo de fotos el algoritmo deberá extraer y agrupar las características y almacenar esta información para su comparación futura. Cabe decir que estas características deben ser muy precisas debido a que, por ejemplo, una mancha o el color de piel son parámetros muy generales para una comparación de una foto de referencia con una foto de prueba.

Debido a que el algoritmo debe extraer las características de la foto y que según sea el caso de la técnica de reconocimiento facial, serán una o varias características, este proceso demanda procesamiento de máquina y un tiempo prudente, sin embargo, cuando hay varias fotos del usuario el algoritmo deberá pasar por cada foto, analizarla y extraer las características, lo cual aumentará considerablemente el procesamiento de cada imagen.

Ahora, si se habla del ingreso de una imagen de prueba al sistema, el algoritmo nuevamente deberá analizarla y extraer las características de esta foto y aparte de eso debe comparar las características extraídas con las ya existentes en el sistema y esto compete a la comparación de cada una de las características de las fotos de los usuarios registrados.

Esto indica el gran trabajo y procesamiento que tiene que hacer la técnica de reconocimiento facial, a la hora de su funcionamiento, por esta razón entre más usuarios haya en el sistema tanto el tamaño de la base de datos como el poder del procesador tiene que incrementar.

Teniendo en cuenta lo anterior para cada locación se debe tener en cuenta un número mínimo y máximo de personas registradas en el sistema, como en este proyecto se habla de hogares y no de empresas, multinacionales, ni sitios con gran número de personal. Teniendo esto claro para los hogares en Colombia se debe estimar un mínimo y un máximo de personas que habitan un solo hogar.

El DANE (Departamento Administrativo Nacional de Estadística)<sup>34</sup> hace una estadística sobre la población en Colombia y sus características es estadística es llamada Censo nacional de población y vivienda Colombia la versión 2018 dictamina que en promedio hay 44,164,417 de personas habitando el país y solo 7,181,469 de personas habitan Bogotá, ahora según en Bogotá del 100% de las viviendas el 92.9% están ocupadas por personas presentes en el hogar, además según esta encuesta el promedio mínimo de personas por hogar en julio del año 2019 es de 3.10 persona por vivienda, lo que aproximaría en gran medida el mínimo de usuarios por vivienda para el funcionamiento del sistema de reconocimiento facial.<sup>35</sup>

Por este motivo el mínimo de usuarios que tendría el sistema serío de 4 personas, debido a que este sistema como cualquier dispositivo tecnológico avanzado requiere actualización o mantenimientos por tal motivo requiriera adicionar un usuario al promedio mínimo de personas por hogar. Este último usuario será administrador con prioridades de configuración del sistema.

Para el máximo de usuario del sistema este estará sujeto a la capacidad de procesamiento del dispositivo que se adquiera y de la base de datos ya que estos son indispensables para que el reconocimiento facial sea eficiente y se ejecute en tiempos razonables.

**8.1.2 Funcionamiento del sistema según el medio o factores externos.** Para el funcionamiento ideal del sistema se debe tener en cuenta algunas características debido a que estas pueden afectar la viabilidad del reconocimiento facial.

**Características de la cámara:** incluso bajo la misma iluminación, la distribución del color de la piel para la misma persona difiere de una cámara a otra dependiendo de las características del sensor de la cámara. El color reproducido por una cámara CCD "(Charge Coupled Device o, en español, Dispositivo de Carga Acoplada) el cual es un tipo de sensor que es sensible a la luz y trabaja a manera de líneas de píxeles con una cobertura de los colores primarios (RGB)"<sup>36</sup> Y estas cámaras dependen de la reflectancia espectral, que prevalece condiciones de iluminación y sensibilidades del sensor de la cámara.

**Etnia:** el color de la piel también varía de una persona a otra debido a que pertenece a diferentes grupos étnicos y de personas de diferentes regiones. Por ejemplo, el

---

<sup>34</sup> DANE. 20 de septiembre de 2019. DANE información para todos, Disponible en: <https://www.dane.gov.co/>

<sup>35</sup> CNPV (Censo Nacional de Población y Vivienda). 2018. "Contexto". DANE. Pag 15

<sup>36</sup> Jaime Medina 18 de abril de 2012. ¿Sensor CCD o CMOS? ¿Qué significa todo esto?, Disponible en: [https://www.parentesis.com/tutoriales/Sensor\\_CCD\\_o\\_CMOS\\_Que\\_significa\\_todo\\_esto](https://www.parentesis.com/tutoriales/Sensor_CCD_o_CMOS_Que_significa_todo_esto)

color de la piel de personas pertenecientes a grupos asiáticos, africanos, caucásicos e hispanos. Es diferente el uno del otro y varía de blanco, amarillo a oscuro, por lo tanto, este cambio afecta el reconocimiento facial y el sistema debe ser capaz de adaptarse a dichos cambios.

**Características individuales:** características individuales como como la edad, el sexo y las partes del cuerpo también afectan el color de la piel apariencia.

**Otros factores:** diferentes factores como la apariencia del sujeto (maquillaje, peinado y gafas), colores de fondo, Las sombras y el movimiento también influyen en la apariencia del color de la piel.

**La variación de iluminación:** Esta una de las características del medio que más afecta al reconocimiento facial, y debido a está, muchos investigadores y científicos buscan la forma de mitigar el efecto dañino que hace la luz para el reconocimiento facial, debido a que es muy difícil identificar patrones o características específicas cuando las tonalidades de la piel o características cambian de color.

Y aunque de cierta manera es practico extraer características deseadas de una imagen bajo un entorno controlado, y a esto se refiere a un entorno con luz controlada fondo uniforme o de una sola tonalidad y solo en el caso de reconocimiento facial por medio de video un entorno donde el usuario este estático, sin embargo si hablamos de reconocimiento bajo un entorno no controlado la cara debe ser reconocida bajo diversos efectos como variaciones o cambio en la distribución de la fuente de luz y en el nivel de iluminación (interior, exterior, reflejos, sombras, luces no blancas) produce un cambio en el color de la piel en la imagen esto es llamado problema de constancia de color o sobreexposición y sub-exposición.

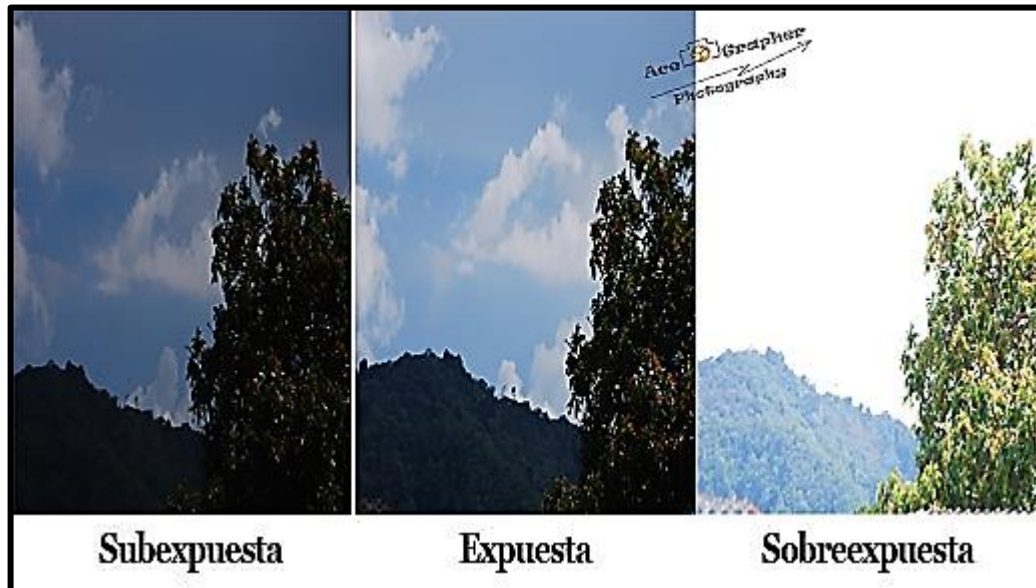
La sobreexposición es un efecto dado a la exposición excesiva de luz sobre un material sensible a la luz que en este caso es la cámara digital, este efecto se da o se produce cuando hay demasiada luz en una fotografía.<sup>37</sup>

La sub-exposición produce un efecto de una imagen demasiado oscura perdiendo detalle en las sombras, que tienen un aspecto negro profundo y carecen de detalle, lo cual afectaría a gran medida la extracción de características para el reconocimiento facial. En la figura 23, se ve un ejemplo claro de este fenómeno y como afecta la calidad de una imagen.

---

<sup>37</sup> P. Kakumanu, S. Makrogiannis, N. Bourbakis. 2007. "A survey of skin-color modeling and detection methods" ITRI/Department of Computer Science and Engineering, Wright State University, Dayton OH 45435, USA. Pág 1. Disponible en : <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.3484&rep=rep1&type=pdf>

Figura 23. Sobreexposición y sub-exposición de una imagen.



Fuente: Ace Grapher, Sobreexposición y sub-exposición de una imagen. subexposición, exposición correcta y sobreexposición. TIPS PARA EL USO DE TU EQUIPO FOTOGRAFICO. 2013. [Consultado: 21 de septiembre de 2019]. Disponible <https://acegrapher.wordpress.com/2013/06/22/subexposicion-exposicion-correcta-y-sobreexposicion>

Para este tipo de fenómenos que ocurren al tomar una foto existen tres métodos que logran disminuir en gran medida estos efectos los cuales son: Nivel de gris la cual hace una transformación de nivel de gris a la imagen para visualizar características relevantes, gradiente la cual se utiliza para extraer bordes de una imagen en nivel de gris y reflejo facial técnica la cual se utiliza para la estimación de campo.

Teniendo en cuenta lo anterior se debe utilizar un algoritmo o técnica de reconocimiento facial que dentro de sus componentes o características este la corrección del efecto de la luz a la que se expondría una foto del usuario cuando llegue a su hogar.

Además de esto se tiene que utilizar una técnica eficiente para efectos del color de la piel y características propias de la persona y para esto se debe tener en cuenta una base de datos robusta para que estas pequeñas variaciones no afectan la funcionalidad del sistemas además de esto es de gran importancia que si el usuario tiene un gran cambio físico en su cara o en su caso, el sistema cambia de usuarios este debe actualizar tanto su algoritmo de entrenamiento como la base de datos que maneje el reconocimiento facial.

Debido al gran número de factores externos que pueden afectar el reconocimiento facial, se recomienda que, para el buen uso del sistema, los usuarios no usen objetos que cubran características faciales importantes, como gafas oscuras o pañoletas, debido a que el sistema no podrá reconocer al usuario y este no permitirá el acceso, esto no incluye las prendas de vestir. En el caso de que el usuario use gafas medicadas, es aconsejable retirarlas ya que el sistema pueda que no lo reconozca con este tipo de objetos.

**8.1.3 Requerimientos.** Los requerimientos son una condición o capacidad que un usuario o sistema necesita para resolver un problema o satisfacer una necesidad y poder lograr un objetivo.

Estos requerimientos están divididos en dos, funcionales y no funcionales. Los funcionales son declaraciones de las funciones que el sistema debe ser capaz de realizar, de cómo debe responder ante las situaciones previstas, mientras que los requerimientos no funcionales, son restricciones del sistema, tales como disponibilidad, mantenimiento, seguridad, capacidad de los dispositivos de entrada/salida, rendimiento (como velocidad y tiempo de respuesta), etc.

En base a estas definiciones, se realizará un análisis de requerimientos con el objetivo de identificar tanto las funcionalidades que se esperan de sistema como sus limitaciones.

#### **8.1.3.1 Requerimientos funcionales.**

- Ingresar un usuario al sistema.
- Capturar una serie de fotos del usuario a través de una cámara con la posibilidad de guardarla en la placa de desarrollo.
- Asignar un espacio de memoria en la base de datos de cada usuario.
- Extraer características de las fotos almacenadas.
- Extraer características de las fotos de entrada.
- Comparar las características de la foto de entrada con las características de cada una de la foto de los usuarios almacenados en la base de datos.
- Identificar a una persona por medio de una imagen de su rostro.
- Permitir o denegar el acceso según sea el porcentaje de similitud.
- Eliminar Usuarios.
- Agregar usuarios.

#### **8.1.3.2 Requerimientos No funcionales.**

- El sistema debe funcionar con una cámara estándar y luz artificial en el caso de las horas nocturnas.

- El sistema debe ejecutarse en tiempo real, lo que implica que la eficiencia de la técnica de reconocimiento facial debe ser alto para que las operaciones computacionales se procesen en un tiempo razonable.
- Las actualizaciones del sistema se llevarán al cabo en tiempos prolongados debido a que la eficiencia del sistema pueda variar con respecto a los cambios físicos del usuario.

## 8.2 ANÁLISIS DEL COMPONENTE FÍSICO

Dado que es un componente vital para que el algoritmo de reconocimiento facial funcione a través de él, es imperativo elegir dispositivos (placa de desarrollo y la cámara fotográfica), lo suficientemente eficaces para hacer uso de los procesos ya definidos, por lo tanto, a continuación, se mencionaran algunas de las placas de desarrollo y cámaras utilizadas para el reconocimiento facial.

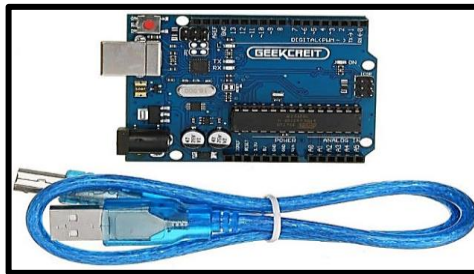
### 8.2.1 Tipos de placa de desarrollo

**Arduino Uno:** Es muy conocido en la industria debido a su popularidad entre los ingenieros ya que es una opción completa para proyectos iniciales con un uso simple de programación, además que posee una inmensa cantidad de librerías las cuales ahorran a gran medida el tiempo de desarrollo.

Aunque no es uno de los más rápidos y es limitado por su número de pines de entradas y salidas, aunque su costo es bastante bajo no son muy adecuados para los proyectos con muchos sensores y/o procesamiento.

En la figura 24 se evidencia la estructura del Arduino UNO donde en los costados se encuentran las entradas input y output, en el lado izquierdo esta la entrada de poder.

Figura 24. Arduino UNO.



**Fuente:** Yúbal FM. Arduino UNO [imagen]. Qué es Arduino, cómo funciona y qué puedes hacer con uno. Xataka Basics. 2019. [Consultado: 26 de septiembre de 2019]. Disponible en: <https://www.xataka.com/basics/que-arduino-como-functiona-que-puedes-hacer-uno>.

Arduino UNO tiene su propio entorno de desarrollo de software de plataforma cruzada llamado Arduino Software IDE. Además, Arduino utiliza lenguaje C lo cual sus programas pueden ser escritos en C o C ++.

Este dispositivo debido a su gran implementación en distintas áreas de estudio es bastante económico debido a su gran popularidad. En el mercado hay gran variedad de estos dispositivos y cada uno con características y uso específicos. En la figura 25 se presenta un cuadro con las características que nos ofrece este dispositivo, tanto en variedades en el mercado, como accesorios, kits, y módulos.

De color verde se evidencia la variedad de dispositivos que tiene Arduino. De color rojo se encuentran los módulos que se puede utilizar junto a los dispositivos Arduino. De color naranja se encuentra los escudos y portadores los cuales adicionan funcionalidades extra. De color café se encuentran los kits que ofrecen en el mercado y por último de color gris los accesorios disponibles para cada funcionalidad de Arduino.

Figura 25. Variedad de dispositivos Arduino y sus herramientas.



Fuente: KNIGHTS KEVIN, Placas de desarrollo que son y por que los necesitas. Roboperks. 2018 [Consultado: 15 de julio de 2019]. Disponible <https://www.roboperks.com/language/es/placas-de-desarrollo/>

**Raspberry Pi:** Este dispositivo funciona como una computadora del tamaño de una tarjeta de crédito y fue desarrollada para enseñar ciencias computacionales, al igual que el Arduino UNO tiene entradas (inputs) y salidas (Outputs) las cuales le permiten ingresar varios sensores o si bien se quiere dispositivos, Como computadoras es mucho más rápida para procesar información a comparación del Arduino, lo que hace que su rango de aplicación sea bastante diverso. Como se evidencia en la figura 26 la Raspberry pi 3 contiene un módulo ethernet y Wifi para conexiones a internet, cuenta con dos entradas USB, y entradas para video e imagen digital, además tiene más de 40 pines para utilizarlos en diferentes aplicaciones.

Figura 26. Raspberry Pi 3 B+.



**Fuente:** Pastor Javier. Raspberry Pi 3 B+ [imagen]. Raspberry Pi 3 Model B+, análisis: más potencia y mejor WiFi para un miniPC que sigue asombrando. Xataka Basics. 2019. [Consultado: 15 de julio de 2019]. Disponible en: <https://www.xataka.com/ordenadores/raspberry-pi-3-model-b-analisis-mas-potencia-y-mejor-wifi-para-un-minipc-que-sigue-asombrando>

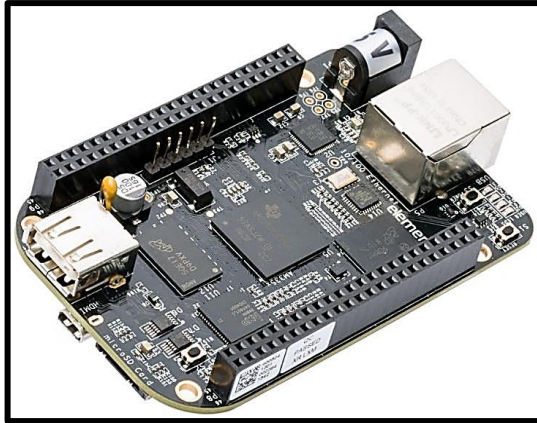
Raspberry Pi 3 modelo B, su sistema operativo es Raspbian (basado en Debian (Linux)), pero también es capaz de ejecutar Android y Microsoft, Sistema operativo Windows 10 IoT. Cualquier idioma que se pueda usar en ARMv8 también puede implementarse en el Raspberry Pi. Tales idiomas incluyen Python, C, C ++, Java, Scratch, y Ruby, siendo Python el más popular. Hay muchas placas de expansión (Shields) para el Raspberry Pi.

**Beaglebone:** Es una pequeña computadora bastante similar a la Raspberry pi como se ilustra en la figura 27, aunque esta difiere de las Raspberry pi en algunos aspectos como:



1. Posee más pines de entrada y salida  
Esto la hace más eficaz al ofrecer gran capacidad de computación sin perder capacidades como lo son el procesamiento y el control.
2. Soporta varios sistemas operativos (S.O)  
Esto quiere decir que puede funcionar con distintos S.O tales como: Android, Ubuntu y otros tipos de Linux.

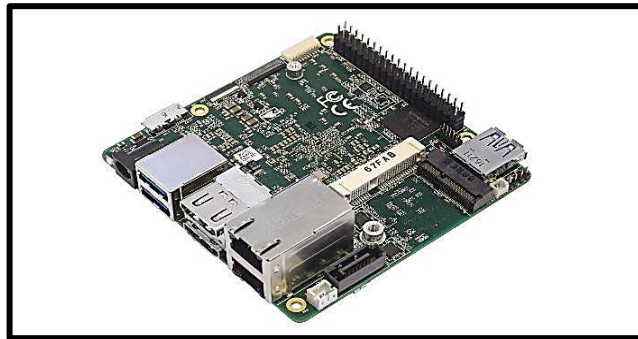
Figura 27. Beaglebone.



**Fuente:** Gizmojo. Beaglebone [imagen]. Beaglebone Black - Rev C. Gizmojo. 2015. [Consultado: 15 de julio de 2019]. Disponible en: <https://www.gizmojo.com.ar/products/beaglebone-black-rev-c>.

**Up square:** Es una placa de desarrollo fabricada por Intel que al igual que las anteriores, es una pequeña computadora, pero en este caso orientada a un propósito totalmente distinto. Ofrece la capacidad de procesar y graficar rápidamente, y también ofrece múltiple entrada para pantalla como se evidencia en la figura 28, está también incluye entradas y salidas que incluso se pueden expandir su número, viene pre instalado para el sistema operativo Ubuntu y posee alrededor de 400 librerías, esta placa tiene un gran potencial en aplicación de inteligencia artificial.

Figura 28. Up square.

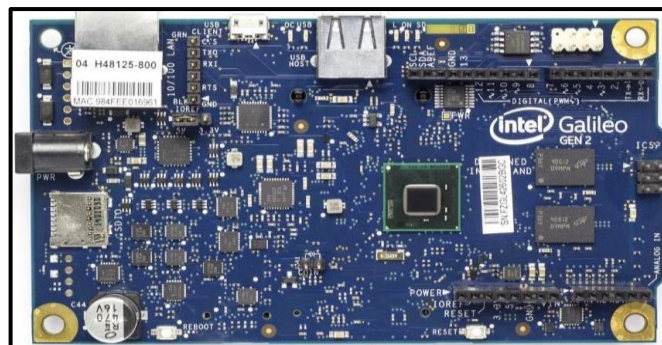


Fuente: Up bridge de gap. Up square [imagen]. UP Squared Specifications. Up square. 2019. [Consultado: 15 de julio de 2019]. Disponible en: <https://up-board.org/upsquared/specifications/>

**Intel Galileo Gen 2:** Es un dispositivo que combina la tecnología de Arduino con Intel ya que es el primer dispositivo que se certifica bajo la arquitectura x86 de Intel, Su uso es educativo para aplicación tecnológicas o proyectos, esta placa de desarrollo utiliza el sistema operativo Linux, su gran ventaja es que puede utilizar la gran variedad de librerías que posee Arduino.<sup>38</sup>

En la figura 29, se ilustra la placa de desarrollo Intel Galileo Gen2.

Figura 29. Intel Galileo Gen 2.

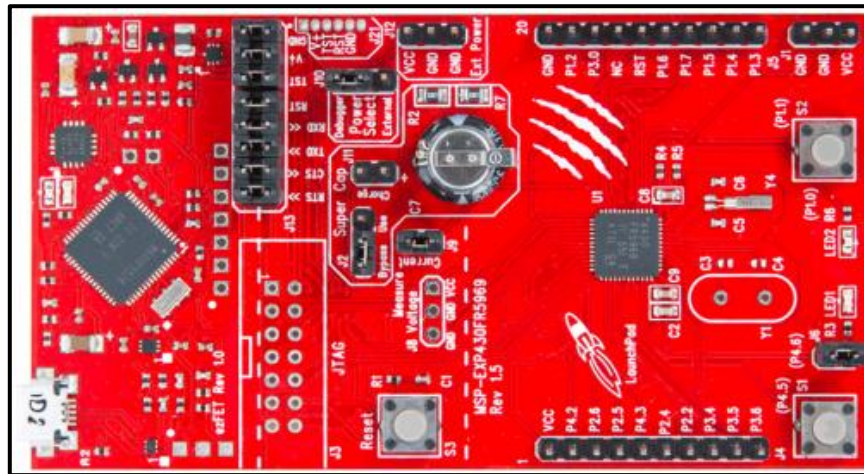


Fuente: INTEL. Intel Galileo Gen 2 [imagen Board Intel® Galileo de segunda generación. INTEL. 2019. [Consultado: 15 de julio de 2019]. Disponible en: <https://ark.intel.com/content/www/es/es/ark/products/83137/intel-galileo-gen-2-board.html>

<sup>38</sup>Intel. Board Intel: Galileo de segunda generación. [Sitio web] [Consultado: 8 de octubre de 2019]. Disponible en: <https://ark.intel.com/content/www/es/es/ark/products/83137/intel-galileo-gen-2-board.html>

**LaunchPad MSP-EXP430FR5969:** Es una placa de desarrollo de micro controlador fácil de usar debido a que está basada en el IDE de Arduino, como se evidencia en la figura 30, cuenta con algunos botones y LED integrados para la integración de una interfaz de usuario simple, así como un SuperCap que permite aplicaciones independientes sin fuente de alimentación externa; También ofrece herramientas de desarrollo gratuitas basadas en la nube para un uso rápido. Todas estas herramientas aceptan código C / C ++ para programar LaunchPad. También se pueden usar otros compiladores de C / C ++.<sup>39</sup>

Figura 30. LaunchPad MSP-EXP430FR5969.



**Fuente:** Texas Instruments. MSP430FR5969 LaunchPad Development Kit [imagen]. Texas Instruments. 2015. [Consultado: 15 de julio de 2019]. Disponible en: <http://www.ti.com/tool/MSP-EXP430FR5969>

**8.2.2 Características de las placas de desarrollo.** Para hacer una selección del dispositivo adecuado se deben comparar varios factores y dispositivos, por esta razón se decide mostrar a continuación en la tabla 3, algunas de las características más relevantes de las placas de desarrollo.

<sup>39</sup> TEXAS INSTRUMENTS, MSP430FR5969 LaunchPad Development Kit [sitio web]. [Consultado: 8 de Octubre de 2019]. Disponible en: <http://www.ti.com/tool/MSP-EXP430FR5969>

Tabla 3. Características principales de cada placa de desarrollo.

PLACA DE DESARROLLO	VOLTAJE DE SALIDA	CONSUMO DE ENERGIA	PINES GPIO	ENTRADA ANALOGA	COSTO (US \$)	COSTO (COP \$)
Raspberry Pi 3 Model B	3.3 V	300 mA -1.34 A	17	NO	35.00	116.705
BeagleBone Black Rev C	3.3 - 5V	210 mA - 460 mA	66	SI	55.00	183.394
Arduino UNO Rev 3	3.3 - 5V	23µA - 45mA	22	SI	24.95	83.194
Intel Galileo Gen 2	3.3 - 5V	379 mA -430m A	20	SI	45.00	150.050
LaunchPad MSP-EXP430FR5969	5V	0,02µA - 100µA	20	SI	15.99	53.317

Fuente: Selecting a development board for your capstone or course proyect. Consultado: 20 de julio de 2019

En la tabla 3, se muestra la comparación con respecto a voltaje de alimentación, consumo de energía, numero de pines (GPIO), costos de algunas placas de desarrollo en dólares. Este costo comparado entre dólares y pesos colombianos está representado por la Tasa representativo del mercado TRM de junio del 2018

Tabla 4. Detalles de audio e imagen.

PLACA DE DESARROLLO	SALIDA DE VIDEO	DSI	CSI	SALIDA DE IMAGEN
Raspberry Pi 3 Model B	HDMI	SI	SI	HDMI/audio jack
BeagleBone Black Rev C	MicroHDMI	NO	NO	MicroHDMI
Arduino UNO Rev 3	NO	NO	NO	NO
Intel Galileo Gen 2	NO	NO	NO	NO
LaunchPad MSP-EXP430FR5969	NO	NO	NO	NO

Fuente: Selecting a development board for your capstone or course proyect. Consultado: 20 de julio de 2019

En la tabla 4, se presentan algunas características de algunos formatos de video que maneja ciertas placas de desarrollo.

Tabla 5. Redes y almacenamiento.

PLACA DE DESARROLLO	ETHERNET	WI-FI	BLUETOOTH	ALMACENAMIENTO EXTERNO	ALMACENAMIENTO INTERNO
Raspberry Pi 3 Model B	SI	SI	SI	MicroSD	NO
BeagleBone Black Rev C	SI	NO <sup>(1)</sup>	NO <sup>(1)</sup>	MicroSD	4GB
Arduino UNO Rev 3	NO	NO <sup>(1)</sup>	NO <sup>(1)</sup>	NO	32KB
Intel Galileo Gen 2	SI	NO <sup>(1)</sup>	NO <sup>(1)</sup>	SD	8MB
LaunchPad MSP-EXP430FR5969	NO	NO <sup>(1)</sup>	NO <sup>(1)</sup>	NO	64KB

Fuente: Selecting a development board for your capstone or course project. Consultado: 20 de julio de 2019

En la tabla 5, se muestran algunas características con respecto al uso de la red dentro del dispositivo esto indica que el dispositivo es capaz de conectarse bajo el protocolo ethernet, wifi y bluetooth, en algunas placas de desarrollo se indica un (No) lo cual identifica que propiamente la placa no tiene esta característica, pero si la placa de desarrollo indica NO<sup>1</sup> esta puede acoplarse con un dispositivo para que cumpla con la característica especificada. Por otro lado, se especifica una característica importante como lo es el almacenamiento interno que ofrece cada dispositivo.

Tabla 6. Software de la placa desarrolladora.

PLACA DE DESARROLLO	CPU	GPU	RAM	SISTEMA OPERATIVO	OPEN SOURCE
Raspberry Pi 3 Model B	ARM Cortex-A53 (1.2 GHz, 4 NUCLEOS )	Broadcom VideoCore IV	1GB	LINUX, Windows 10	PARCIALMENTE
BeagleBone Black Rev C	ARM Cortex-A8 (1 GHz, 1 NUCLEO )	PowerVR SGX530	512 MB	LINUX, Android	PARCIALMENTE
Arduino UNO Rev 3	Atmel AT-mega328P (16MHz, UN NUCLEO)	NO	2KB	NO	SI
Intel Galileo Gen 2	Intel Quark x 1000 (400MHz, UN NUCLEO)	NO	256 MB	LINUX	PARCIALMENTE
LaunchPad MSP-EXP430FR5969	MSP-430FR5969, 16-bit (16MHz UN NUCLEO)	NO	2KB	NO	SI

Fuente: Selecting a development board for your capstone or course project. Consultado: 20 de julio de 2019

En la tabla 6 se muestran las características más específicas de cada placa de desarrollo como qué tipo de unidad central de procesamiento utiliza, que unidad de procesamiento gráfico usa, cual es la capacidad de memoria de acceso aleatorio, el sistema operativo que maneja, y si es de uso libre.

**8.2.3 Tipos y características de cámaras de reconocimiento facial.** La cámara es parte fundamental del sistema, ya que esta es la que toma las fotos del usuario. Debido a que hay bastantes cámaras que se utilizan para el reconocimiento facial, a continuación, se recopila información de algunas de ellas con sus características.

**8.2.3.1 Módulo de cámara V2 Raspberry Pi.** Es un módulo para la placa Raspberry Pi, una cámara de alta definición (HD) y se conecta a cualquier Raspberry Pi, este módulo se utiliza para crear fotografías y vídeo HD.

#### Características

- Imágenes de alta calidad (3280 px por 2464 px)
- Alta capacidad de datos.
- Enfoque fijo de 8 megapíxeles.
- Compatible con 1080p30, 720p60 y VGA90.

- Sensor de imagen CMOS Sony IMX219PQ.
- Cable plano de 15 contactos.

**8.2.3.2 Kinect.** Esta es una cámara que utiliza el Xbox 360<sup>40</sup> y viene integrada con sensores de movimiento haciendo que el usuario que la utilice pueda interactuar con el xbox sin ningún dispositivo extra (véase figura 31) .

### Características

- Las cámaras tienen dos resoluciones, 320x240 y 640x480 de alto color.
- Enviar datos con una frecuencia de actualización de 30 fps.
- Cuenta con una cámara RGB.
- Sensor de profundidad.
- Micrófono multi-array.
- Procesador que proporciona captura de movimiento de todo el cuerpo en 3D, reconocimiento facial y capacidades de reconocimiento de voz.
- Campo de visión.
  - Campo de visión horizontal: 57 grados.
  - Campo de visión vertical: 43 grados.
  - Rango de inclinación física:  $\pm 27$  grados.
  - Rango de profundidad del sensor: 1,2 – 3,5 metros.

Figura 31. Sensor Kinect.

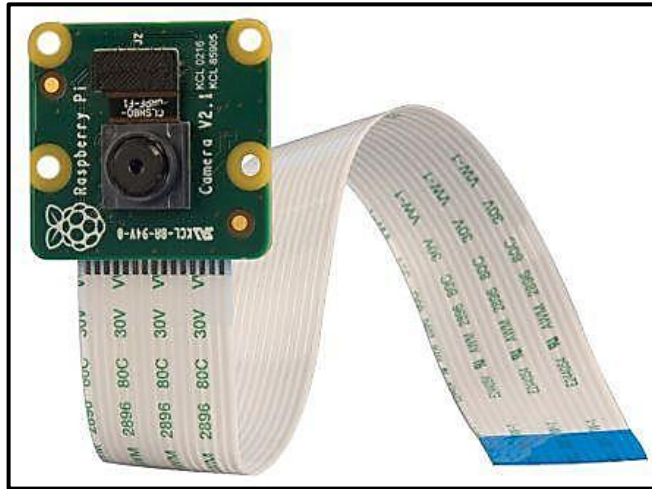


Fuente: [www.microsoft.com.co](http://www.microsoft.com.co). Consultado: 23 de julio de 2019.

<sup>40</sup> Microsoft. 2019. "Kinect" [sitio web]. [Consultado: 20 de octubre de 2019]. Disponible en: <https://www.xbox.com/es-CO/>

**8.2.3.3 Sony IMX219PQ.** Alta sensibilidad y alta velocidad en los 8 megapíxeles en el campo de visión completa y 30 imágenes por segundo, también es posible obtener imágenes 4 veces más rápidas mediante el modo de agrupamiento analógico  $2 \times 2$ .<sup>41</sup> Como se evidencia en la figura 32, esta cámara es bastante versátil debido a sus dimensiones y su gran poder de procesamiento de imagen.

Figura 32. Cámara V2 Raspberry Pi.



Fuente: Brico Geek. Cámara Raspberry Pi v2 - 8 Megapixels [imagen]. 2017. [Consultado: 15 de julio de 2019]. Disponible en: <https://tienda.bricogeek.com/accesorios-raspberry-pi/822-camara-raspberry-pi-v2-8-megapixels.html>

#### **8.2.3.4 Cámara AXIS P1354.** Cámara de sistema de seguridad<sup>42</sup>

Es una cámara de seguridad la cual se ilustra en la figura 33, donde tiene una gran longitud de foco grabar y tomar fotos en grandes distancias.

##### **Características**

- Sensor Progressive scan RGB CMOS 1/3.
- Iluminación Color: 0.1 lux, F1.2, B/W: 0.02 lux, F1.2.
- Tecnología Lightfinder: Alto rendimiento en condiciones de iluminación difíciles.
- Almacenamiento local.
- Pan-tilt-zoom digital (PTZ), inclinación de la cámara con enfoque.

<sup>41</sup> Sony, Semiconductor Solutions Corporation. 2014. "IMX219PQ". [sitio web]. [Consultado: 22 de octubre de 2019]. Disponible en: [https://www.sony-semicon.co.jp/products\\_en/new\\_pro/april\\_2014/imx219\\_e.html](https://www.sony-semicon.co.jp/products_en/new_pro/april_2014/imx219_e.html)

<sup>42</sup> Axis.com 2019. "AXIS P1354" [sitio web]. [Consultado: 22 de octubre de 2019] Disponible en: <https://www.axis.com/es-ec/products/axis-p1354>



Figura 33. Cámara AXIS P1354.



Fuente: [www.axis.com](http://www.axis.com). Consultado: 23 de julio de 2019.

**8.2.3.5 ECAM 8000.** Esta es una cámara de alta definición que tiene gran nitidez, y reduce el efecto de contraluz utilizando WDR (Wide Dynamic Range), esta cámara como se evidencia en la figura 34, tiene una gran amplitud en el lente lo cual le permite mucho más ingreso de luz en las imágenes.

#### **Características**

- Unidad de sensor CMOS de píxeles de alta definición 720p.
- Lente de foco fijo.
- Formato de archivo MPEG/WMV.
- Micrófono Digital Sí.
- Resolución (DPI) 2MP, 1920 x 1080, 1280 x 720, 640 x 480 píxeles.
- Resolución de video CIF / VGA: hasta 30fps / 720p HD: hasta 30 fps / 1080P hasta 30 fps.
- Ángulo de visión, arriba y abajo de 90 ° / 360 ° de rotación.
- UVC (Plug & Play).
- Peso 82 g (Incluye clip y cable).
- Dimensiones (A x A x P) 54,5 x 90,6 x 67,5 mm (2,15 x 3,57 x 2,66 pulgadas).<sup>43</sup>

---

<sup>43</sup> HOSPITAL del trabajador. 2018. "Ergonomía: adaptando el trabajo a las personas". [Sitio web], [Consultado el 28 de Octubre de 2019] Disponible en: "<https://www.hospitaldeltrabajador.cl/ht/Comunidad/GuiaSalud/Salud/Paginas/Ergonomia.aspx>"

Figura 34. Cámara ECAM8000.



Fuente: Genius. ECam 8000 Full definición alta 1080p. [imagen]. 2019. [Consultado: 21 de mayo de 2019.]. Disponible en: <http://pe.geniusnet.com/product/ecam-8000>

### 8.3 ANÁLISIS DEL ALGORITMO

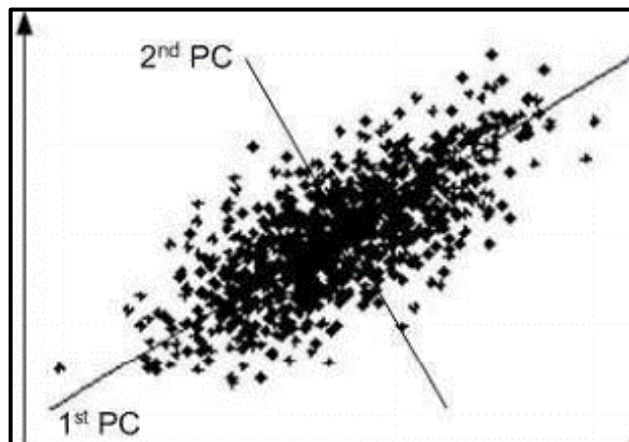
El análisis del algoritmo es propiamente la implementación de la técnica de reconocimiento facial en forma matemática, por esta razón es esencial saber las propiedades de cada técnica y sus características. Esto quiere decir que el algoritmo hace el procesamiento de imagen, extracción de características y comparación en la base de datos, por lo tanto, la técnica debe ser lo suficientemente eficaz y precisa para responder a las necesidades del usuario. Por esta razón a continuación se recopila información sobre las técnicas de reconocimiento facial más comunes en el mercado.

**8.3.1 Técnicas de reconocimiento facial.** Algunas de las técnicas de reconocimiento más utilizadas en la literatura se describen a continuación.

**8.3.1.1 Análisis de componentes principales (pca).** Este análisis de componentes es un método para representar de forma eficiente un conjunto de puntos de muestra, haciendo esto reduce la dimensionalidad de la descripción (imagen) proyectando los puntos los ejes principales, donde un conjunto de ejes orto normales está mayormente en la matriz de dirección de covarianza máxima de datos. Estos vectores explican mejor la distribución de imágenes faciales ya que PCA minimiza la proyección cuadrada mediante un error para un número dado de dimensiones, también proporciona una medida de importancia (en términos de total error de proyección) para cada eje.<sup>44</sup>

Este método está basado en la transformada de Karhunen-Loeve (KLT), la cual consiste en la representación de un proceso estocástico no periódico, a lo cual indica un proceso probabilístico que usa magnitudes aleatorias que varían en el tiempo para caracterizar una sucesión de variables, y esto lo hace a través de una base de vectores obtenidos. Esto indica de cierta forma que este método permite representar una imagen de una cara usando como base la observación de varias caras.

Figura 35. Componentes principales de un conjunto de puntos bidimensional.

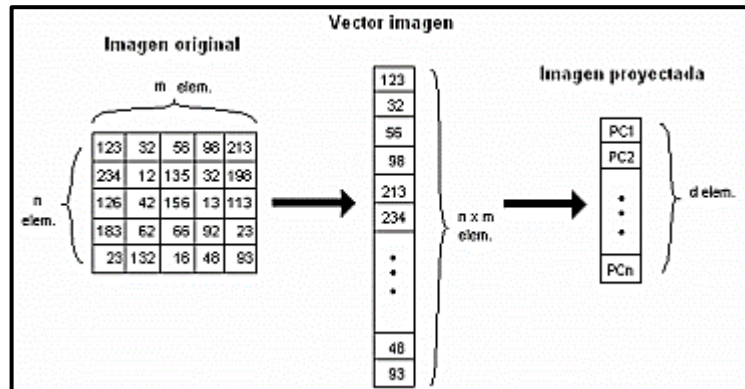


Fuente: Estudio de técnicas de reconocimiento facial. Consultado: 19 de agosto de 2019

En la figura 35, la primera componente ofrece una reducción lineal óptima de dimensión de 2D a 1D en cuanto a error cuadrático medio se refiere. La reducción dimensional que realiza este método es equivalente al número de auto vector que se utilice. Como se muestra la figura 36.

<sup>44</sup> Delac, K., M. Grgic, and P. Liatsis. 2008. "Appearance-Based Statistical Methods for Face Recognition," no. June: 151–58. <https://doi.org/10.1109/elmar.2005.193665>.

Figura 36. Ejemplo de reducción dimensional al aplicar PCA.



Fuente: Estudio de técnicas de reconocimiento facial. Consultado: 19 de agosto de 2019

**8.3.1.2 Análisis discriminante lineal (LDA).** Este es un método para el reconocimiento de patrones y aprendizaje de máquina no supervisado, y se usa para encontrar una combinación lineal de rasgos que caracterizan dos o más clases de objetos. Al combinar estos objetos su resultante podría ser un clasificador lineal.

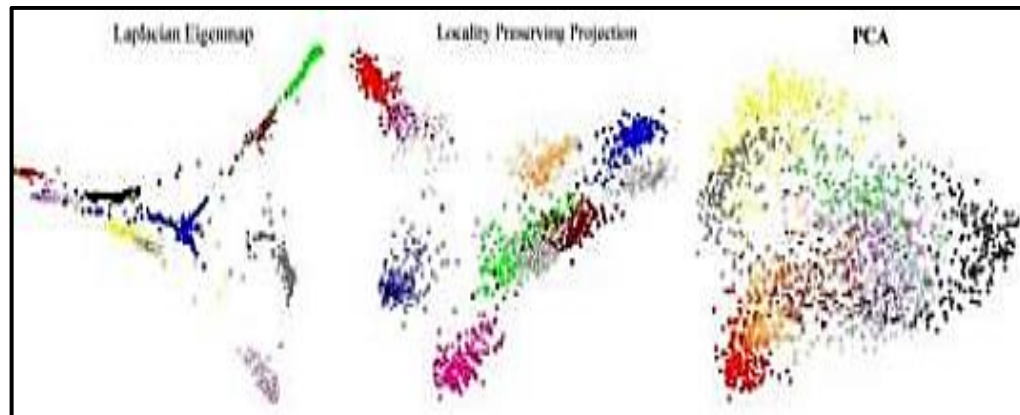
Este método tiene como objetivo convertir el problema de la alta dimensionalidad en uno de baja, para ello el LDA proyecta las imágenes en un espacio vectorial de baja dimensionalidad de forma que la relación cuantificada entre las dos clases y la distancia dentro de la clase se maximiza.

**8.3.1.3 Proyecciones de preservación local (LPP).** LPP es un algoritmo lineal PCA el cual realiza una reducción dimensional de los datos. Al tratarse de un algoritmo lineal es rápido y útil para aplicaciones prácticas.

Una de sus propiedades es que en vez de conservar la estructura de todos los datos como lo hacía en PCA este, solo conserva los datos de estructura local, de este modo los datos cercanos o comúnmente llamado “vecinos” serán los mismos en el espacio original, además de esto al conservar una estructura local de los datos de una misma imagen los patrones más referentes estarán muy cercanas y alejadas de otros parámetros o clases.

En la figura 37 se evidencia las diferencias que hay en cuanto a la agrupación de los datos según la técnica utilizadas.

Figura 37. Diferencia de PCA en LPP.



Fuente: Estudio de técnicas de reconocimiento facial. Consultado: 19 de agosto de 2019

**8.3.1.4 Transformada discreta de coseno (DCT).** Es una transformación que representa en forma de una secuencia finita los datos como unas series de sumas de funciones cosenoidales oscilando a diferentes frecuencias.

Este método además de ser utilizado en reconocimiento fácil tiene grandes aplicaciones como procesamiento de señales compresión de audio e imágenes hasta métodos espectrales. A diferencia del PCA este método no necesita estar entrenado con imágenes del mismo tipo, solo se transforman las imágenes directamente en información y se compara, la gran ventaja de este método es su bajo coste computacional con relación al PCA.<sup>45</sup>

**8.3.1.5 Algoritmo de viola-jones.** Es un método de detección de objetos se destaca por su bajo costo computacional, lo que permite que sea empleado en tiempo real.

Su desarrollo fue motivado por el problema de la detección de caras, donde sigue siendo utilizado, pero puede aplicarse a otras clases de objetos que, como las caras, estén caracterizados por patrones típicos de iluminación.

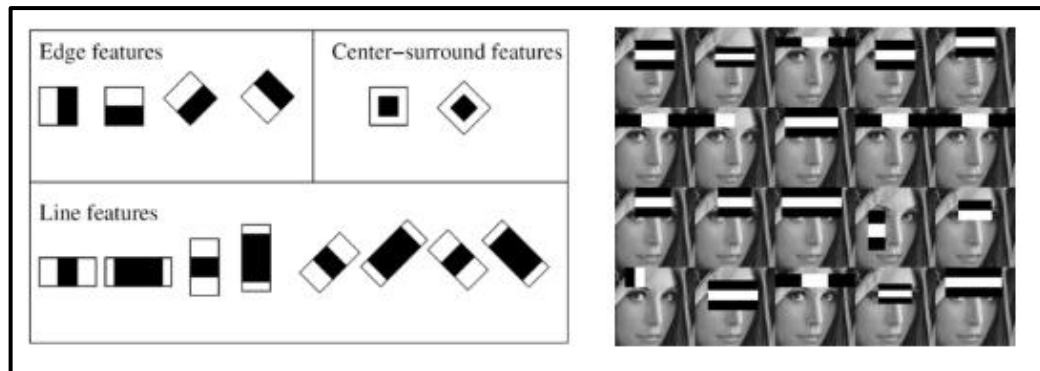
Se basa en una serie de clasificadores llamados Haar-like features que se pueden calcular eficientemente a partir de una imagen integral, se agrupan en una cascada empleando un algoritmo de aprendizaje basado en AdaBoost para conseguir un alto rendimiento en la detección, así como una alta capacidad discriminativa en las primeras etapas.

---

<sup>45</sup> Hernández, Roger Gimeno. 2010. "Estudio De Técnicas De Reconocimiento Facial." Información Tecnológica Pag. 19-28.

Existen tres tipos de características de este algoritmo y son representadas en la figura 38, en la parte izquierda, mientras que en la parte derecha se puede observar algunos ejemplos de características Haar comunes de un detector de caras. Este algoritmo considera regiones rectangulares en una ventana de detección, suma las intensidades de los píxeles en cada región y calcula la diferencia entre estas sumas.

Figura 38. Método de clasificación de Viola-Jones.



Fuente: Métodos para reconocimiento facial. Consultado: 19 de agosto de 2019

**Haar-like features.** Son los elementos básicos con los que se realiza la detección. Estos clasificadores son características muy simples que se buscan en las imágenes y que consisten en la diferencia de intensidades luminosas entre regiones rectangulares adyacentes. Las características quedan por tanto definidas por unos rectángulos y su posición relativa a la ventana de búsqueda y adquieren un valor numérico resultado de la comparación que evalúan.

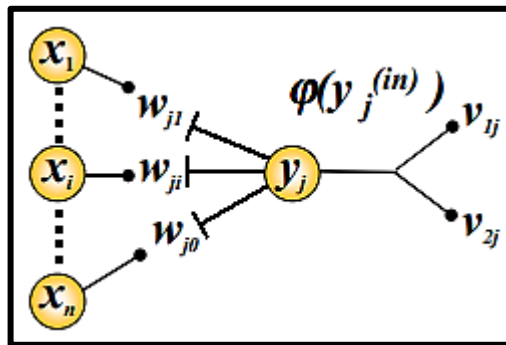
**8.3.1.6 Eigen-Face.** Eigenface es una técnica de reconocimiento facial y una representación de imagen facial, donde los vectores ortonormales se combina de forma lineal. Las imágenes tratadas por esta técnica, se obtienen de los vectores de la matriz de covarianza por medio del conjunto de imágenes almacenadas en una base de datos, donde  $i_1, i_2, \dots, i_k$  son un conjunto de imágenes faciales ( $k$ ), y cada una se ordena lexicográficamente.

Los vectores de la matriz  $L$  (son los grandes), estos tienen un subespacio lineal y pueden reconstruir la imagen de la cara con el mínimo error de reconstrucción en el sentido de los mínimos cuadrados.

**8.3.1.7 Redes neuronales artificiales.** Las redes neuronales artificiales es una de las técnicas para reconocimiento facial. Existen modelos que se utilizan para construir neuronas con el fin de modelar correctamente el comportamiento global de toda la red, teniendo en cuenta que no se desea igualar el comportamiento fisiológico de la neurona, sino se desea modelar las características más importantes para que estas se tengan en cuenta al momento que se hace la unión a la red neuronal.

En la figura 39, se evidencia el esquema de la neurona, donde se muestra la neurona de interés que es la  $y$ , las neuronas  $x$ , son las que envían señales de entrada y se pueden ver como valores numéricos, los valores  $w$ , representan los pesos sinápticos en las dendritas de  $y$ .

Figura 39. Esquema neuronal.



Fuente: Redes neuronales: Funciones en base radial (RBF)

**8.3.1.8 Gabor Feature.** Se basa en la utilización de filtros, aplica 40 filtros Gabor diferentes en una imagen, como resultado se reciben 40 imágenes con diferentes ángulos y orientaciones, luego se calculan los puntos de intensidad máxima en cada imagen filtrada y se marcan como puntos fiduciales. El sistema reduce estos puntos de acuerdo a la distancia entre ellos, después se calculan las distancias entre puntos reducidos utilizando fórmula de distancia, por último, las distancias se comparan con la base de datos y si coinciden significa que se detectan las interfaces en la imagen.<sup>46</sup>

<sup>46</sup> Modi, Mitul, and Fedrik Macwan. 2014. "Face Detection Approaches: A Survey." International Journal of Innovative Research in Science, Engineering and Technology 3 (4): 11112–16 Pag 11109. [www.ijirset.com](http://www.ijirset.com)

**8.3.2 Observación del comportamiento de las técnicas de reconocimiento facial.** En este subcapítulo se compararon varias técnicas de reconocimiento facial respecto a su precisión utilizando bases de datos disponibles en el mercado.

En la tabla 7, compara métodos de reconocimiento facial como PCA, LDA, DCT, ICA, donde las imágenes o fotos de los usuarios están con cierta variación de pose, esto quiere decir que los usuarios hacen un gesto la cual en la base de datos no está registrada.

Tabla 7. Exactitud de los algoritmos de reconocimiento facial frente a la variación de la pose.

Estrategia	Resultados	
	Metodo	Tasa de reconocimiento %
Uso de cinco imágenes de cada persona para el entrenamiento de cinco imágenes de	PCA	68/100 =68,00
	LDA	60/100 =60,00
	DCT	67/100 =67,00
	ICA	60/100 =60,00

Fuente: A Comparative Study of Face Recognition under Pose Variation.

En la tabla 8, se hacen pruebas de reconocimiento facial entre los métodos PCA y LDA comparando su funcionamiento con características propias de un entorno no controlado como condición de iluminación, el uso del vidrio como reflejo, y las expresiones faciales, cabe aclarar que para cada característica hay un número de imágenes de prueba diferente.

Tabla 8. Resultados de los experimentos (12).

Categoría de imágenes	No. total de imágenes de prueba	No. De cara reconocido PCA	No. De cara reconocida LDA	Tasa de reconocimiento facial en PCA (%)	Tasa de reconocimiento facial en LDA (%)
Condición de iluminación	45	25	22	55,55	48,88
Vidrio-Non Vidrio	30	25	28	83,33	93,33
Expresion Facial	90	70	70	77,77	81,21
Todas las imágenes	165	120	123	72,72	74,47

Fuente: A Comparative Study of Face Recognition under Pose Variation.<sup>47</sup>

En la tabla 9, se hace una comparación de las técnicas faciales basadas en Eigen faces propuestas por varios autores y utilizando distintas bases de datos ubicadas en la red, para cada técnica utilizada se expresa la precisión que tiene esta, utilizando distancia entre los puntos en comparación de las imágenes.

<sup>47</sup> Shinwari, Ali Rehman. 2019. "A Comparative Study of Face Recognition under Pose Variation," 137–41.



Tabla 9. Comparación de las técnicas de reconocimiento facial basadas en EigenFace.

Metodos	Año	Base de datos	Tecnicas	Presición		
				No. De Principales Componentes	Euclidean Distancia	Manhattan Distancia
Slavković et al	2012	ORL Face Database	PCA Eigen Faces	5	77.5%	80%
				20	97.5%	97.5%
				190	97.5%	97.5%
Rahman, ArmanadurniAbd, et al	2014	-	PCA Eigen Faces	70%		
Saha, Rajib et al.	2013	FRAV Face Database	Eigen Face	96%		
Thakur, S., et al.	2008	AT&T Face Database, UMIST Face Database	PCA, RBF NN	94.10%		
Abdullah et al.	2012	Face94	PCA	100% i.e. 0% FAR		
Aishwarya, P. et al.	2010	RICE Face Database	Multiple Eigenface Subspaces	94.8%		
Rizon, Mohamed, et al.	2006	ORL Face Database	Eigenface, BackpropagationNN	-		
Agarwal, Mayank, et al.	2010	Olivetti Face Database, ORL Face Database	PCA, Feed Forward Back Propagation NN	97,018%		
Gupta, Sheifali, et al.	2010	ORL Face Database	Eigen Face	97%		

Fuente: Face Recognition: A Survey.

En la tabla 10, se hace una comparación de los enfoques que se le puede dar a la técnica de reconocimiento facial llamada Gabor, esta es propuesta por varios autores en sus respectivos años. Estos autores utilizaron al igual que en la tabla anterior base de datos diferentes ubicadas en la red.

Tabla 10. Comparación de los enfoques de reconocimiento facial basados en Gabor Wavelet.

Metodos	Año	Base de datos	Técnicas	Presición		
				No. De Principales Componentes	Euclidean Distancia	Manhattan Distancia
Slavković et al	2012	ORL Face Database	PCA Eigen Faces	5	77.5%	80%
				20	97.5%	97.5%
				190	97.5%	97.5%
Rahman, ArmanadurniAbd, et al	2014	-	PCA Eigen Faces	70%		
Saha, Rajib et al.	2013	FRAV Face Database	Eigen Face	96%		
Thakur, S., et al.	2008	AT&T Face Database, UMIST Face Database	PCA, RBF NN	94.10%		
Abdullah et al.	2012	Face94	PCA	100% i.e. 0% FAR		
Aishwarya, P. et al.	2010	RICE Face Database	Multiple Eigenface Subspaces	94.8%		
			Eigenface,			
Rizon, Mohamed, et al.	2006	ORL Face Database	BackpropagationNN			
			PCA, Feed Forward			
Agarwal, Mayank, et al.	2010	Olivetti Face Database, ORL Face Database	Back Propagation NN	97,018%		
Gupta, Shaifali et al.	2010	ORL Face Database	Eigen Face	97%		

Fuente: Face Recognition: A Survey.

En la tabla 11, se hace una comparación de las técnicas faciales basadas en Redes neuronales propuestas por varios autores y utilizando distintas bases de datos ubicadas en la red, para cada técnica utilizada se expresa el porcentaje de precisión que tienen.

Tabla 11. Comparación de técnicas de clasificación en base a la red neuronal.

Metodos	Años	Base de datos	Tecnicas	Tasa de Reconocimiento %	
Nazeer et al. [86]	2007	-	Histogram Equalization, Homomorphic Filtering, PCA, LDA, ANN Euclidean Distance, Normalized Correlation	Extractor de características PCA	Tasa de reconocimiento
					91.85%
					91.85%
					92.59%
				LDA	90.00%
					92.22%
					85.56%
Toh, Soon Lee et al. [88]	2003	Japanese Face Image Database	Resource Allocating Network with Long-Term Memory (RAN-LTM), Incremental Linear Ability	-	
Ghassabeh et al. [89]	2007	Yale Face Database BioID	Incremental LDA, APCA Network	-	
Vinitha, K. V. et al. [90]	2009	Face Database	Probabilistic Neural Network, Template Matching Method, Voronoi Tessellations	-	
Nagi, Jawad et al. [91]	2008	-	2D-Discrete Cosine Transform (2D-DCT), SOM	81.36%	
Mantri, Shamla et al. [93]	2011	AT & T Database	SOM	92.40%	
Raja, A. S. et al. [94]	2012	IIT-Dehli Database	Neural Network Based SOM for Face recognition	88.25% to 98.3%	
Nandini, M. et al. [95]	2013	-	Back Propagation Networks (BPC), Radial Basis Function (RBC) Network		Tasa de reconocimiento
					96,66%
					98,88%
Radha, V. et al. [96]	2011	ORL face Database	RBC Network, Linear Discriminant, Analysis (LDA), Curvelet Transform		
Prasad, M. S. R. S., et al. [99]	2011	Yale Face Database	PCA, FFNN	90% Relacion de aceptación	

Fuente: Face Recognition: A Survey.

En la tabla 12, se hace una comparación de identificación de rostros en secuencia de video utilizando técnicas de reconocimiento facial basadas en la modelo de Markov, al igual que en las anteriores los autores utilizan distintas bases de datos, para ver el comportamiento de sus técnicas

Tabla 12. Comparación de la identificación de las caras de una secuencia de video basada en el modelo oculto de Markov.

Metodos	Años	Base de datos	Técnicas	Presición			
Salah, Albert Ali, et al.	2007	BANCA face Database	Gabor Wavelet Filter, DCT	Tamaño de ventana	Tasa de reconocimiento	Tasa máxima de reconocimiento	
			Compression Feature, HMM, Gaussian	13	95,23%	96.15%	
			Observation Distribution	15	96.85%	98.08%	
				17	93.15%	95.00%	
Ojo, John Adedapo et al.	2011	AT&T Face Database	2D-Discrete Wavelet Transform, HMM	90%			
Miar-Naimi, H.et al.	2008	ORL Face Database	7 State HMM, Quantized Singular Values Decomposition (SVD)	100%			
Bicego, Manuele et al.	2003	ORL Face Database	HMM, Wavelet Coding				
				100%			
Chien, Jen-Tzung et al.	2008	GTFD Face Database, FERET Database	Maximum Confidence HMM				
				95,60%			
Liao, Chih-Pin et al.	2006	ORL Face Database, FERET Face Database	Baseline HMM, Maximum Confidence HMM	Baseline HMM		MCHMM	
				95,50%		97%	
Nicholl, P., et al.	2008	AT & T Database, Essex Faces95 Database, FERET Database	Discrete Wavelet Transform, Haar Wavelet, Gabor Wavelet, Coiflet Wavelet, Structural HMM		97%		
Liu, Xiaoming et al.	2003	Task Database, Mobo Database	Adaptive HMM	Base de datos	Tasa de reconocimiento		
		Modelo temporal de Markov			HMM		
		Task Database			98,40%	98,80%	
		Mobo Database			93%	97%	
Sharif, Muhammad, et, al	2013	ORL Face Database, Yale Face Database	Sub-Holistic HMM	ORL database		Yale Database	
				Resolución	Tasa de reconocimiento	Resolución	Tasa de reconocimiento
				112x92	99,50%	163x240	99,39%
				37x23	98,75%	100x100	98,78%
				18x15	92,25%	30x30	94,54%

Fuente: Face Recognition: A Survey.

En la tabla 13, se hace una comparación de métodos de clasificación basados en SVM (Maquina de vector soporte) el cual arroja el porcentaje de precisión bajo unas bases de datos ubicadas en la red.

Tabla 13. Comparación de métodos de clasificación basados en SVM.

Methods	Year	Database	Methods	Recognition Rate %			
Déniz, Oscar et al. [118]	2003	Yale Face Database, AR Face Database		Base de datos	SVM usando las funciones del kernel		
			ICA, SVM		p=1	p=3	Gaussaian
				Yale	99,39%	99,39%	99,39%
				AR	93,33%	92,67%	94%
Kong, Rui et al. [120]	2011	ORL Face Database	ICA, SVM	96%			
Le, Thai Hoang et al. [123]	2011	FERET Database, AT&T Database		95,10%			
			2D-Principal Component Analysis, SVM				
Smith, Raymond S., et al. [124]	2006	XM2VTS Face Database	Angular- Linear	-			
			Discriminant Analysis (ALDA), SVM				
Jianhong, Xie. Et al. [126]	2008	ORL Face Database	Kernel PCA, LS-SVM	95%			
Xie, Jianhong et al. [127]	2009	ORL Face Database	Curvelet Transform, Least	96%			
			Square Support Vector Machine (LS-SVM)				
Zhang, Xinming et al. [128]	2008	-	Component Base Support	98%			
			Vector Machine				

Fuente: Face Recognition: A Survey. <sup>48</sup>

**8.3.3 Bases de datos para el reconocimiento facial.** Para el reconocimiento facial se utilizan varios métodos y técnicas, de la cuales ya se han hablado, pero también existen un tipo de almacenamiento de rostros, llamados bases de datos de

<sup>48</sup> Article, Review, Muhammad Sharif, Farah Naz, Mussarat Yasmin, Muhammad Alyas Shahid, and Amjad Rehman. 2017. "Face Recognition: A Survey" 10 (2): 166–77.

reconocimiento facial, algunas son libres para descargar, algunas generan costo y otras no están disponibles por motivos de seguridad como la del gobierno, estas se pueden utilizar de forma académica, cultural, seguridad, entre otras, a continuación, se nombren algunas bases de datos.

- Interpol.
- Google.
- Amazon.
- AT&T.
- Gobiernos nacionales e internacionales.
- Muchas empresas que a nivel mundial tienen sistemas de reconocimiento facial interno también tienen su base de datos con rostros.

Sin embargo, para este proyecto la base de datos que se utilizó es una propia, debido a que el algoritmo fue entrenado con las mismas fotos del usuario, gracias a esto se ahorra tiempo y dinero.

## 9. DEFINICIÓN DE REQUERIMIENTOS

En este capítulo contiene los requerimientos necesarios para la implementación del sistema de reconocimiento facial. Estos requerimientos ayudaron en gran medida a escoger tanto el dispositivo indicado, el software y técnica más eficiente para realizar el proyecto.

Dentro de estos requerimientos se encuentran los de unidad de procesamiento, cámara, algoritmo, y software.

### 9.1 REQUERIMIENTOS DE LA UNIDAD DE PROCESAMIENTO

Algunos de los parámetros o requerimientos que requiere el sistema son los siguientes.

- CPU y velocidad de reloj: Esto afecta a gran medida el rendimiento en general de la placa y es la que define que tan veloz es la placa para ejecutar cálculos.
- RAM: Esta variable afecta el número de tareas que se pueden ejecutar simultáneamente. También afecta la rapidez con la que los datos se pueden procesar, como el intercambio de datos de RAM a no volátil el almacenamiento incurre en un gran rendimiento y gastos generales.
- UNIDAD DE PROCESAMIENTO GRÁFICO: Una unidad de procesamiento gráfico (GPU) permitirá a la placa de desarrollo ejecutar salida de video (VGA, HDMI, etc.). Una GPU de alto rendimiento es lo más necesario al procesar video e imágenes con la placa de desarrollo.
- ALMACENAMIENTO: El almacenamiento afecta el tamaño de los programas, sistemas operativos y datos generados o descargados que pueden almacenarse en una placa de desarrollo.
- NÚMERO DE PINES DE I/O PARA UN PROPÓSITO EN GENERAL: Se utilizan para conectar componentes a la placa de desarrollo; por lo tanto, más pines típicamente significa más componentes conectados simultáneamente.
- OPEN-SOURCE: Open source hardware association es un código abierto, como tener un diseño que cualquier dispositivo y que esta se pueda hacer, modificar, distribuir y usar. El software asociado con el hardware debe estar suficientemente documentado para escribir software de código abierto o estar bajo una licencia aprobada por open-source. Una placa de desarrollo se etiquetará "parcialmente código abierto" si solo se incluye en la definición de hardware o la definición de software.
- CONSUMO DE ENERGÍA: Este puede jugar un papel importante en las elecciones de diseño. Para proyectos portátiles, o proyectos que necesariamente necesiten una fuente de poder continua, para esto se debe considerar primero

los requisitos de tiempo de ejecución y el poder de mando de la placa, también componentes asociados al seleccionar una fuente energética.

Ahora bien, teniendo en cuenta los parámetros planteados, se decidió por usar una placa de desarrollo con un gran procesamiento a la hora de ejecutar algoritmos y programas bastante robustos, debido a que el reconocimiento de cada imagen demanda bastante procesamiento y de igual forma se quiere una placa de desarrollo con bastante memoria RAM ya que se ejecutaran varias tareas al mismo tiempo lo que agilizaría el proceso en tiempos y ejecución.

Además de eso se busca una placa de desarrollo con bastante capacidad de almacenamiento, ya que en esta se piensa almacenar las imágenes de referencia, para la debida comparación de la imagen de entrada o usuario. Aparte de esto se busca de cierta forma minimizar lo más posible los costos y que su uso sea de forma gratuita.

## **9.2 REQUERIMIENTOS DE LA CÁMARA**

Los requerimientos de la cámara son esenciales ya que estos permitieron tener un concepto más allá de solo tomar una imagen, Estos conceptos ayudaron a tener una mejor perspectiva para el mejoramiento de la imagen del usuario, y como facilitar la captura de imagen con buena calidad para el debido procesamiento. Una de estos conceptos es la ergonomía.

### **9.2.1 Ergonomía**

Uno de los principales problemas a los que se enfrenta los sistemas de reconocimiento facial es la ubicación de las cámaras, debido a que en muchos casos la altura o el ángulo donde se encuentra la cámara no es el más adecuado o la cámara no cuenta con tecnologías que eviten el contraste de la luz o incluso la resolución del dispositivo no es muy buena.

La ergonomía es el estudio que utiliza conocimientos científicos para que los sistemas, productos o el ambiente se adapten a las condiciones físicas o mentales del ser humano. Por esta razón el componente principal de la ergonomía está centrada en las personas y en como acondicionar un ambiente de trabajo para el confort y eficiencia productiva tanto del sistema como el de la persona.<sup>49</sup>

Para este proyecto la ergonomía tiene como objetivo identificar y adaptar el sistema de reconocimiento facial, en un lugar específico para que cumpla con las

---

<sup>49</sup> HOSPITAL del trabajador. 2018. "Ergonomía: adaptando el trabajo a las personas". [Sitio web]. [Consultado el 2 de noviembre de 2019]. Disponible en: <https://www.hospitaldeltrabajador.cl/ht/Comunidad/GuiaSalud/Salud/Paginas/Ergonomia.aspx>



condiciones de trabajo y las características del usuario que en este caso es la altura del usuario. Además, establecer las condiciones ergonómicas para la adquisición de nuevas herramientas de trabajo como lo es la cámara implementada en el sistema.

Para esto se han puesto unos criterios indispensables para que el sistema sea ergonómico y eficaz a la hora de identificar al usuario y brinde confort a la hora de utilizarlo.

**Altura.** Este aspecto puede ayudar en gran medida a la eficiencia del reconocimiento facial, si se coloca de manera correcta, debido a que en general estas cámaras de reconocimiento facial son colocadas a una altura considerable, es de vital importancia saber el verdadero uso que se les dará. Un ejemplo de esto son las cámaras de seguridad que por su uso están colocadas a una altura no mínimo de 2.20 metros, y están colocadas en las esquinas de las paredes para abarcar más campo de visión.

Para este proyecto la cámara tiene que ser colocada en una altura de tal forma que el sistema brinde confort y a la misma vez sea eficiente haciendo que su tiempo de procesamiento sea mínimo. Teniendo esto claro, lo ideal sería instalar el sistema de reconocimiento facial teniendo en cuenta la altura de las personas que residen en el hogar, dando así un sistema, que se adapte a las condiciones de los habitantes de cada hogar.

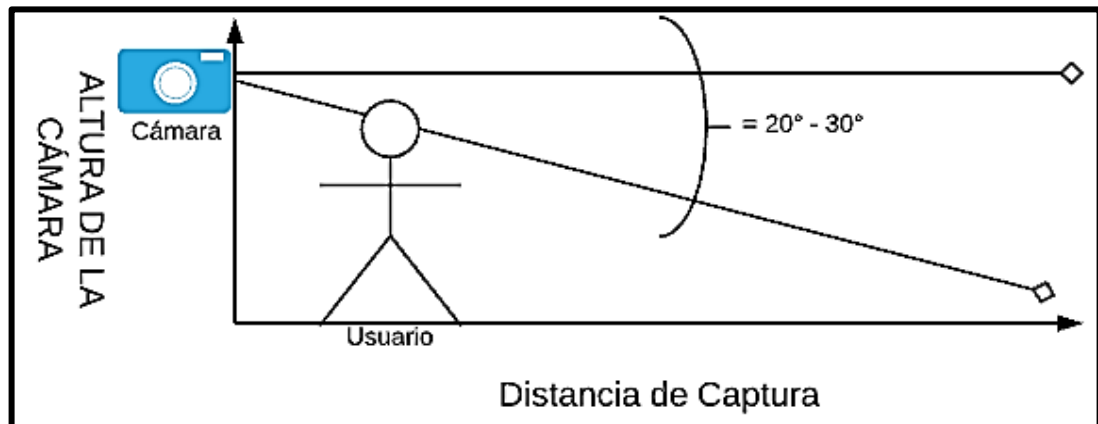
**Resolución de la cámara.** Al tomar una foto por medio de una cámara, esta tendrá una resolución alta o baja y eso dependerá del número de píxeles de ancho por el número de píxeles de alto. La alta definición HD (1920x1080 píxeles) permite imágenes nítidas, donde claramente se pueden ver características faciales del usuario. Si bien se sabe la imagen donde se encuentra el rostro, esté solo será una parte de la foto entera, a lo que equivale a un número determinado de píxeles, si se tiene en cuenta la escala donde se toma la foto, es evidente que entre más lejos se tome la foto del rostro del usuario, esta ocupará menos espacio dentro de la foto, por lo tanto, habrá menos píxeles y la resolución disminuiría drásticamente; Lo que afectaría en gran medida el reconocimiento facial.

Debido este problema se es necesario una cámara con una resolución alta para que el algoritmo capte el rostro y extraiga sus características sin importar la distancia, claro está que debe ser una distancia prudente a la cual la cámara en cuestión detecte el rostro.

**Angulo de inclinación.** Este es un factor bastante clave, debido a que la mayoría de sistemas de reconocimiento facial trabajan de manera óptima si la cámara es ubicada en un ángulo de inclinación de entre  $20^\circ$  y  $30^\circ$ .<sup>50</sup>

La instalación ideal de la cámara de reconocimiento facial está definida como se ilustra en la figura 40.

Figura 40. Posición de la cámara.



Fuente: Autores. Hecho: 9/10/2019

En ángulo de instalación de la cámara como se evidencia en la figura # depende de las características propias de cada hogar, por esta razón se dan las pautas, Donde la distancia de captura es inversamente proporcional a la nitidez de la foto del rostro en la imagen, por tal motivo se tiene que tomar la foto en un rango prudente.

La altura de la instalación de la cámara tiene que ser a una medida superior a la altura promedio de las personas que residen en un hogar.

**Contraste.** El contraste es un problema recurrente en las cámaras que se destinan para el control de acceso, debido a que este contraste es generado por la luz del exterior e impide el reconocimiento facial haciendo que la imagen tomada se oscurezca. Este inconveniente, aunque difícil de evitar y poco se puede hacer con respecto a la luz del exterior. Se puede utilizar tecnologías que recurran a la misma luz para que modifiquen de cierta forma la imagen y la hagan parecer más clara, un ejemplo es el WDR (amplio rango dinámico). Esta tecnología permite ajustar de manera automática la luminosidad de una imagen cuando el lugar presenta bastante luz, disminuyendo en gran medida el contraste.

<sup>50</sup> PDI, Policía de investigaciones de Chile. Guía para el buen uso de sistemas de cámaras de seguridad. Capítulo 1: Sistema de reconocimiento facial. Chile. Pág 9. **Disponible en:** [camaras-seguridad%20ergonomia.pdfG](#)

### **9.3 REQUERIMIENTOS DEL ALGORITMO**

Los requerimientos del algoritmo dieron las pautas para escoger la técnica de reconocimiento facial ideal, ya que esta comprende desde la detección del rostro hasta la comparación y clasificación de la foto. Por lo tanto, este análisis se hizo desde enfoques diferentes, debido a que se tiene que identificar las características ideales y no ideales del comportamiento del algoritmo en entornos controlados y no controlados.

Para esto, se hizo una lista de requerimientos esenciales del algoritmo:

- Capacidad de detectar un rostro
- La eficiencia del algoritmo con cierto número de usuarios.
- La capacidad del algoritmo al reaccionar al contraste de la luz natural.
- Influencia en la variación de aspectos de la cara.
- Eficiencia computacional con respecto a los recursos que utiliza el algoritmo.
- Tiempo de ejecución y respuesta.

### **9.4 REQUERIMIENTOS DEL SOFTWARE**

El software es donde se realiza las tareas demandas por el algoritmo. Por esta razón es muy importante saber que requerimientos tiene el sistema con respecto al software, dado que estos requerimientos de software son características que debe tener el software instalado en el dispositivo. Estos requerimientos pueden ser de sistema operativo o aplicaciones instaladas.

Los requerimientos con respecto al sistema operativo y de las aplicaciones instaladas van enfocados al uso de software Open Source debido, al costo extra que generaría la adquisición de un software en el mercado.

Además, el software debe ser compatible con la placa de desarrollo y con sus requerimientos, por esta razón se debe tener cuidado con que programa, aplicación, sistema operativo y hasta el lenguaje de programación se utiliza en este proyecto.

## 10. SELECCIÓN DE LAS HERRAMIENTAS DEL SISTEMA10.1 HERRAMIENTAS HARDWARE

Los requerimientos anteriormente mencionados son fundamentales para la realización del proyecto, por esta razón aspectos como el almacenamiento de información haciendo las veces de base de datos. Capacidad de procesamiento el cual debe ser esencial para un funcionamiento ideal, adaptación de una cámara digital otorgada por algunas librerías, el ensamblaje de dispositivos a una placa de desarrollo y además de eso, el bajo costo que debe tener el proyecto.

Con esto aclarado y obteniendo todas las características de cada placa de desarrollo que anteriormente se evidenció, se pasó a escoger la placa de desarrollo, la cual contenga la mayoría de las características de las condiciones previstas para este proyecto. Y con esto se decide que la placa de desarrollo ideal es la Raspberry Pi modelo B +, debido a su gran procesamiento y su gran capacidad de memoria RAM lo cual mejoraría en gran medida el procesamiento, que, aunque no tiene memoria interna lo cual sería bastante indispensable para el almacenamiento de imágenes, esta placa de desarrollo contiene un apartado para introducir una memoria externa lo cual facilita algunos procesos.

Además de eso, aunque no está dentro de los dispositivos más económicos su costo es relativamente bajo debido a su capacidad y teniendo en cuenta, en si es **open source**, supone en gran medida utilizar la parte gratuita para no generar dificultades futuras a la hora de utilizarlo para este proyecto. Además de esto la Raspberry Pi 3 b + tiene una gran ventaja en cuanto a las otras placas debido a su gran número de librerías y dispositivos que funciona como herramientas junto a esta placa. El caso es para la utilización de una cámara, y esta placa tiene bastante forma de utilizar una cámara digital como medio de entrada de información y según el apartado de **(Marco de referencia, tipos de cámara)** el módulo de cámara V2 Raspberry Pi 3 b es compatible con esta placa.

Con respecto a la cámara, la cual es la entrada de datos al sistema otorgando fotografías de los usuarios para su reconocimiento facial. También se tuvieron en cuenta los requerimientos de la cámara como la resolución en píxeles, tecnologías como CCD o CMOS, incluso la capacidad de mitigar o disminuir el ruido de la imagen y el contraste de la luz con la ayuda del WDR. En este caso se escogió una cámara Full HD llamada ECam 8000 de la marca Genius.

Y por último está el dispositivo encargado de ofrecer al usuario una interfaz gráfica, la cual dispondrá al usuario de varias opciones que contempla el sistema, como: guardar y eliminar usuarios, acceder al sistema o al hogar. Esta dispositivo o pantalla LCD de 3.5 pulgadas está dotada para funcionar directamente con la placa de desarrollo Raspberry pi 3 b +, además, de tener una función de pantalla táctil ideal para el confort del usuario.

## 10.2 HERRAMIENTAS DE SOFTWARE

Los requerimientos del algoritmo anteriormente mencionados son fundamentales para la realización del proyecto, por esta razón aspectos como la técnica de reconocimiento, el software a utilizar, el lenguaje de programación, las librerías que se utilizaron deben ser Open source.

Ahora, debido a que se utilizó la placa ordenadora Raspberry pi, esta dispone de una distribución Linux basada en Debian, el cual es un sistema operativo. Y para instalarlo se utilizó una distribución de Debían especialmente para Raspberry pi, la cual es Raspbian.

El lenguaje de programación que se utilizó para el proyecto es Python, debido a que en la actualidad es muy popular y ha sido utilizado para grandes proyectos. Además, de ser un lenguaje de programación totalmente gratuito ya que su código es totalmente abierto, esto quiere decir que está a disposición del público y no permite vulneraciones al trabajo del programador y su propiedad.

Python también es multiparadigma y multiplataforma, esto quiere decir que es versátil para hacer proyectos, sea para sitios web o inteligencia artificial, Es tal que Python permite desarrollar bajo paradigmas de programación avanzados, tales como:

- Desarrollo de páginas web.
- Desarrollo de diseño y gráficos.
- Aplicaciones financieras.
- Desarrollo de Videojuegos.
- Desarrollo de software.

Ahora bien, para realizar el reconocimiento facial se ha utilizado la herramienta OpenCV, Esta herramienta es muy útil debido a que es una biblioteca o librería de visión artificial (Rama de la inteligencia artificial), esto quiere decir visión por ordenador y permite el análisis de imagen y aprendizaje automático, usando una infinidad de algoritmos para identificar y reconocer los objetos que se decidan. Esta biblioteca es multiplataforma lo que significa que puede ejecutarse en diferentes sistemas operativos como: Windows, iOS, Mac OS, Android y Linux; Y también se puede utilizar en diferentes lenguajes de programación como: Java, Objective C, C#, Python, siendo este último del interés del proyecto. Además de esto este software es totalmente libre, como sus siglas lo indican “OpenCV” (Open Source Computer Vision).

Para el desarrollo de la interfaz del sistema se ha utilizado tKinter para Python el cual es una biblioteca grafica tipo GUI (interfaz gráfica de usuario), y se ha escogido debido a que es estándar en el lenguaje de programación Python y este viene por defecto en la instalación.

Ahora la técnica que se escogió en este proyecto es Eigen-faces, debido a su alta eficiencia con respecto a otros algoritmos y su gran poder a la hora de controlar ciertas perturbaciones en ambientes no controlados, esto se puede revisar en el capítulo “Recopilación de información”

### 10.3 SELECCIÓN DE LA TÉCNICA DE RECONOCIMIENTO FACIAL

La técnica que se ha escogido es Eigenfaces, debido a su gran eficiencia a la hora de procesar imágenes y extrae sus características, además, de su baja tasa de error. Por esta razón se indago un poco más sobre el funcionamiento que tiene esta técnica de reconocimiento facial y como puede junto con otras técnicas trabajar para mejorar en gran medida la eficacia del algoritmo

**10.3.1 Eigen-Faces.** En un principio este término que también se puede ver como una técnica de reconocimiento facial, hace referencia a la visión que tiene un computador hacia el usuario (exterior). EigenFace es un conjunto de vectores propios, por lo cual se puede ver que la palabra completa al momento de desglosarla significa conjunto de vectores aplicados a la cara, ya que el rostro tiene ciertos vectores y ángulos, de esta forma se concluye a un reconocimiento facial mediante esta técnica.<sup>51</sup>

Una gran característica de este término en el campo del reconocimiento facial, es que, al momento de tener un grupo de imágenes ya integrados en una base de datos, Eigen agrupa estas imágenes en una dimensión mucho más pequeña, facilitando la lectura o la comparación al momento de ser necesario para el algoritmo.

Como se había dicho, Eigen, es un conjunto de vectores y estos vectores con las imágenes en conjunto son el resultado de una matriz de covarianza de la distribución de probabilidad sobre el espacio vectorial de alta dimensionalidad de las imágenes de la cara.

Existe un proceso matemático que es el análisis de componentes principales (PCA por sus siglas en inglés), gracias a este proceso EigenFaces se puede tornar como conjunto de imágenes de distintas caras humanas.

El análisis de componentes principales (PCA) se puede ver como una técnica de proyección sub-espacial ampliamente utilizado para el reconocimiento facial, por esta razón va de la mano con Eigenfaces, PCA se encarga de encontrar un conjunto de vectores de proyección más representativos de la muestra original para que así las muestras que se visualizan tengan una gran parte de la información de las

---

<sup>51</sup> Alberto, and Jerónimo Ríos. 2017. “Reconocimiento Facial Por El Método De Eigenfaces.” Pistas Educativas 127 (04): 66–81. Disponible en: <http://itcelaya.edu.mx/ojs/index.php/pistas>.

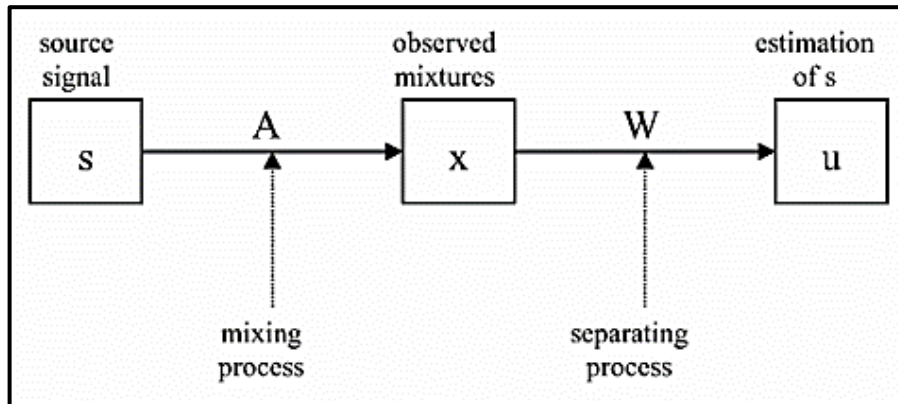
muestras originales, estos vectores más representativos son los más grandes valores de la matriz de covarianza, por otro lado también se habla de otros métodos como el análisis de componentes independientes (ICA) y el análisis discriminantes lineales (LDA), los cuales se describirán a continuación.

- Análisis de componentes principales (PCA). Este análisis de componentes es un método para representar de forma eficiente un conjunto de puntos de muestra, haciendo esto reduce la dimensionalidad de la descripción (imagen) proyectando los puntos los ejes principales, donde un conjunto de ejes ortonormales está mayormente en la matriz de dirección de covarianza máxima de datos. Estos vectores explican mejor la distribución de imágenes faciales ya que PCA minimiza la proyección cuadrada mediante un error para un número dado de dimensiones, también proporciona una medida de importancia (en términos de total error de proyección) para cada eje.<sup>52</sup>
- Análisis de componentes independientes (ICA). PCA se basa en la distribución de probabilidades de los datos de entrada que deben ser gaussianos, en resumen, este método solamente se preocupa por las estadísticas de segundo orden que son la varianza, pero puede fallar en el momento que las variaciones más grandes no corresponden a ejes más significativos de PCA. Mientras que ICA, minimiza el segundo orden y el orden superior lo mantiene dependiendo de la entrada, también mantiene la suposición de linealidad, y aunque ya no usa ciertas cosas de PCA como lo es el espectro de amplitud en el segundo orden, si queda la fase de espectro que se encuentra en las estadísticas del orden superior y estas contienen información estructural en imágenes que impulsan la percepción humana. ICA es una forma de encontrar líneas no ortogonales de un sistema de coordenadas en cualquier dato multivariante, donde las dos direcciones de los ejes del sistema de coordenadas son determinados tanto por el segundo orden como por el superior. El objetivo es hacer una transformación lineal, donde el resultado de las variables y de las estadísticas sea independientes entre sí, a continuación, en la figura 41, se demuestra esto en un diagrama de bloques.

---

<sup>52</sup> Delac, K., M. Grgic, and P. Liatsis. 2008. "Appearance-Based Statistical Methods for Face Recognition," no. June: 151–58. Disponible en: <https://doi.org/10.1109/elmar.2005.193665>.

Figura 41. Diagrama de bloques de las señales independientes.



Fuente: Appearance-Based Statistical Methods for Face Recognition. Consultado: 19 de agosto de 2019

- Análisis discriminante lineal (LDA) o Discriminador lineal de Fisher (FLD). Realizando una comparación entre las anteriores técnicas de reconocimiento facial ICA y PCA, estas dos no usan la clasificación de rostro, mientras que LDA si la usa, ya que encuentra una manera eficiente de representar el espacio vectorial de la cara o del rostro.<sup>53</sup>

**10.3.1.1 Comparación de desempeño (PCA, ICA y LDA).** Las tres técnicas la clasificación se realiza proyectando primero las imágenes de entrada en un sub-espacio a través de una matriz de proyección y luego se realiza la comparación entre el vector de coeficiente de proyección de entrada y todos los vectores de proyección pre-almacenados, también llamados clases etiquetadas, esto para determinar la etiqueta de la clase de entrada.

Se han realizado varias pruebas y testeos para estas técnicas entre varios artículos de grupos de investigación de IEEE, Universidades como Cambridge, revistas científicas internacionales como Reconocimiento de patrones artificiales inteligentes, entre otros, las cuales se encuentran simplificadas en la tabla 14, así mismo las ventajas y desventajas en la tabla 15.

<sup>53</sup> Delac, K., M. Grgic, and P. Liatsis. 2008. "Appearance-Based Statistical Methods for Face Recognition," no. June: 151–58. Disponible en: <https://doi.org/10.1109/elmar.2005.193665>.



Tabla 14. Resultados informados por diferentes grupos de investigación que prueban los tres algoritmos descritos.

<b>Grupo de investigación</b>	<b>Base de datos</b>	<b>Algoritmo probado</b>	<b>Mejor resultado</b>
Zhao	FERET & USC	LDA y PCA+LDA	PCA+LDA
Belhemur	Harvard & Yale	Correlación, Sub-espacio lineal, PCA y LDA	LDA
Navarrete	FERET & Yale	PCA, LDA y EP	LDA
Baveridge	FERET	PCA y PCA+LDA	PCA
Bartlett	FERET	ICA y PCA	ICA
Baek	FERET	ICA y PCA	PCA
Liu	FERET	PCA, ICA y LDA	ICA

Fuente: Appearance-Based Statistical Methods for Face Recognition. Consultado: 19 de agosto de 2019

Tabla 15. Ventajas de Eigenfaces y sus técnicas.

Ventajas de Eigenfaces y sus técnicas	
Eigenfaces	Los datos sin procesar se utilizan directamente para el aprendizaje y el reconocimiento sin ningún procesamiento
	No se requiere conocimiento de la reflexión y la geometría de las caras.
	El reconocimiento es simple y efectivo.
PCA	El reconocimiento es simple y efectivo en comparación con otros enfoques coincidentes
	PCA relaciona completamente cualquier dato en el dominio de transformación
	La compresión de datos se logra mediante la representación de sub-espacio de baja dimensión
	Los datos sin procesar se utilizan directamente para el aprendizaje y el reconocimiento sin ningún procesamiento de nivel bajo o medio.
	No se requiere conocimiento de geometría y transparencia de caras.
	Reduce la entropía total de los datos.
LDA	El LDA maximiza la relación entre la dispersión de clase y la dispersión dentro de clase para resolver el problema de iluminación.
	PCA optimiza la representación de objetos de baja dimensión al enfocarse en características discriminativas, pero la LDA simplemente logra la reconstrucción de objetos.
	LDA funciona da una mejor precisión en la expresión facial.
ICA	ICA proporcionó una representación de datos más poderosa que PCA.
	PCA_ICA attains higher average success rate than Eigenfaces, the Fisher face and methods
	ICA proporcionó una representación de datos más poderosa ya que su objetivo es proporcionar una descomposición y representación de imagen independiente en lugar de no correlacionada. 54

Fuente: Appearance-Based Statistical Methods for Face Recognition. Consultado: 21 de septiembre de 2019

## 11.IMPLEMENTACIÓN DEL PROTOTIPO

Según lo planteado en la metodología este proyecto se basa en un desarrollo en cascada, el cual es un modelo lineal donde se plantea una serie de procesos secuenciales para llegar a un objetivo final. Este objetivo final como bien se sabe, es la implementación de un sistema de reconocimiento facial para el control de acceso en el hogar, el cual tiene unas especificaciones y requerimientos. En este capítulo se tomaron todas las consideraciones de los capítulos anteriormente descritos para la implementación de dicho sistema.

Para el desarrollo de este sistema se necesitaron varias herramientas las cuales ayudaron en gran proporción a realizarlo. Estas herramientas de software y de hardware tienen que ajustarse a las condiciones establecidas en el apartado de requerimientos, además, de tener en cuentas las condiciones típicas de acceso a la vivienda.

Una de estas herramientas es la de hardware, el cual ya se habló en el apartado anterior y se aclaró lo indispensable del uso de dispositivos que cumplan con los requerimientos mínimos, y para esto se tuvieron en cuenta una lista de dispositivos los cuales cumplen con características diferentes y se concluyó lo siguiente:

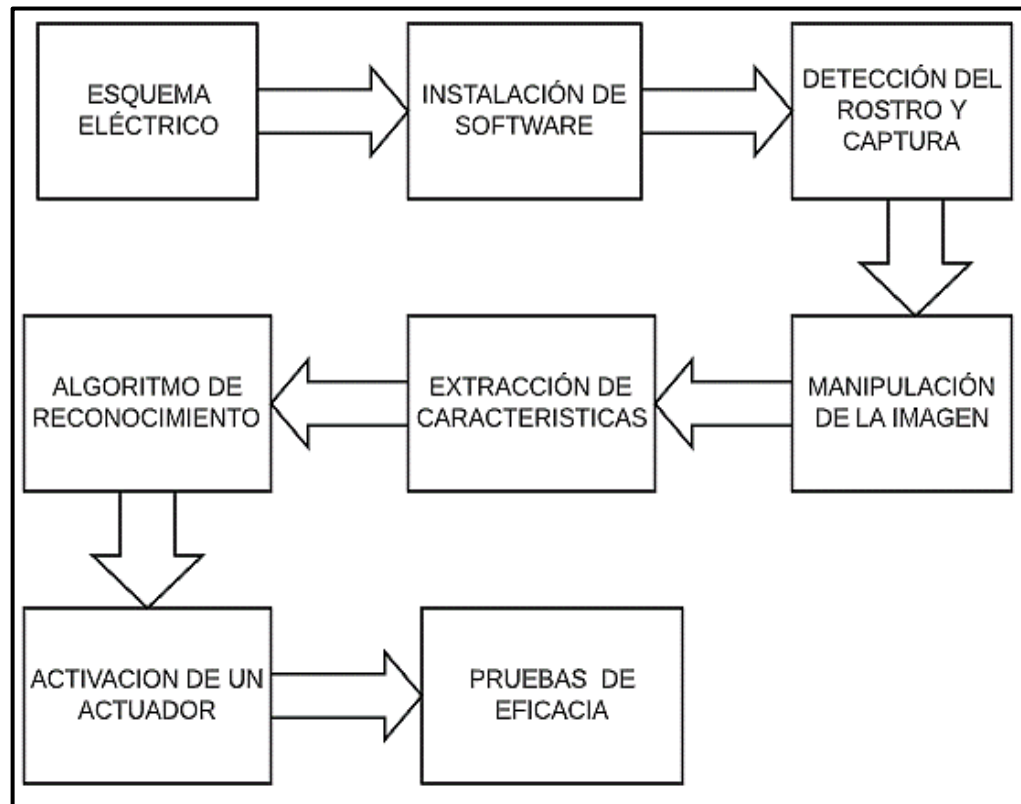
- La placa de desarrollo Raspberry pi 3 B+ es el ideal para el sistema a desarrollar.
- La cámara ECam 8000 cumple con los requerimientos necesarios.
- Dispositivo encargado de ofrecer la interfaz de usuario, es una pantalla LCD de 3.5 pulgadas compatible con Raspberry pi 3 B+.

Las herramientas de software o desarrollo, son utilizadas para crear programas informáticos que a su vez tienen una finalidad, como por ejemplo una aplicación. Estas herramientas deben poseer características compatibles con la placa ordenadora Raspberry pi 3 B+, por esta razón se concluyó lo siguiente:

- Se usó el sistema operativo Linux distribución Debían, ideal para la Raspberry pi 3 B+.
- El lenguaje de programación que se utilizó es Python versión 3.
- Para la realización de los algoritmos se utilizó OpenCV versión 3.2.0.
- Para el desarrollo de la interfaz del sistema se ha utilizado tKinter para Python.
- La técnica que se escogió en este proyecto es Eigen-faces, ya que cumple con los requerimientos necesarios.

Ahora para una buena implementación del sistema se propuso seguir una serie de pasos que conduzcan de una manera ordenada y eficiente el proyecto, estos pasos se evidencian en la figura 42, donde de manera muy característica se define el desarrollo de la implementación del sistema.

Figura 42. Proceso de implementación del proyecto.

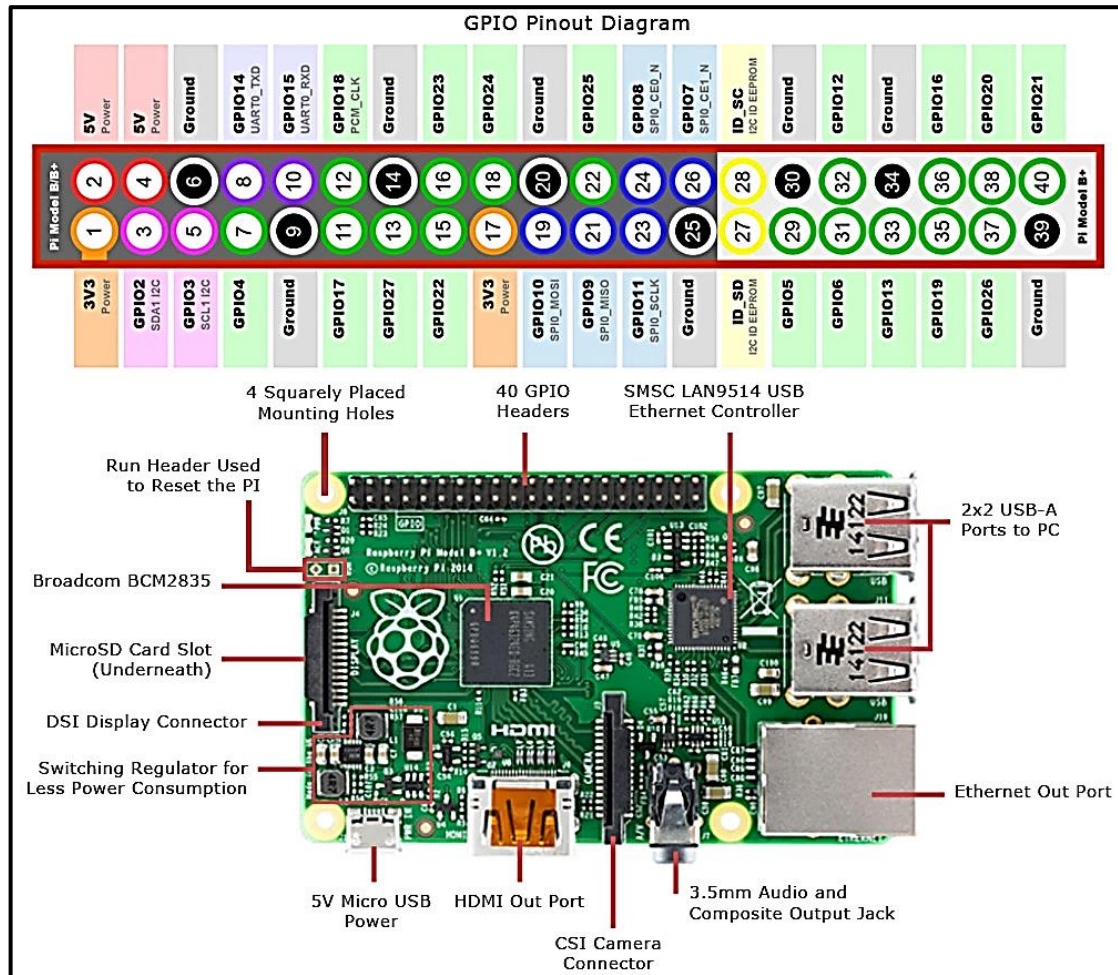


Fuente: Autores. Hecho: 7/11/2019

### 11.1 ESQUEMA ELÉCTRICO

El esquema eléctrico es el apartado donde se identificó las partes físicas que componen el proyecto y como conectarlas entre sí para el debido funcionamiento. Para esto es necesario saber que componentes contiene la Raspberry pi 3 B+, en la figura 43, se muestra el diagrama de la Raspberry pi 3 B+ con sus puertos y funcionalidades.

Figura 43. Diagrama de Raspberry pi 3 B+.



Fuente: Control de GPIO con Python en Raspberry Pi [imagen]. PROGRAMA ERGO SUM. 2019. [Consultado: 9 DE Noviembre de 2019]. Disponible en: <https://www.programoergosum.com/cursos-online/raspberry-pi/238-control-de-gpio-con-python-en-raspberry-pi/intermitente>

En la parte superior de la Figura 43, se muestra el diagrama de pines que tiene la Raspberry pi 3B, estos pines son los que se utilizaron para conectar la pantalla LCD un FAN (ventilador de 5 voltios) y un actuador. También se puede observar varias entradas en las que permiten las entrada de imagen y video sin embargo para este proyecto como se utilizó la cámara ECAM 8000, esta tiene conexión USB, el cual se encuentra en la esquina superior derecha de la Raspberry pi 3B, también se puede observar a un costado la entrada de la tarjeta MicroSD, donde está ubicado el sistema operativo del proyecto y a su vez almacenara las imágenes de los usuarios en una base de datos, y por último en la esquina inferior izquierda está

ubicada la entrada de alimentación proporcionada por un conector micro USB de 5 voltios.

La pantalla Táctil de 3.5 pulgadas tiene unos puertos exclusivos que se conectan a la Raspberry pi 3 estos se ilustran en la figura 44; estos a su vez se conectan con los puertos GPIO de la Raspberry pi 3 B+.

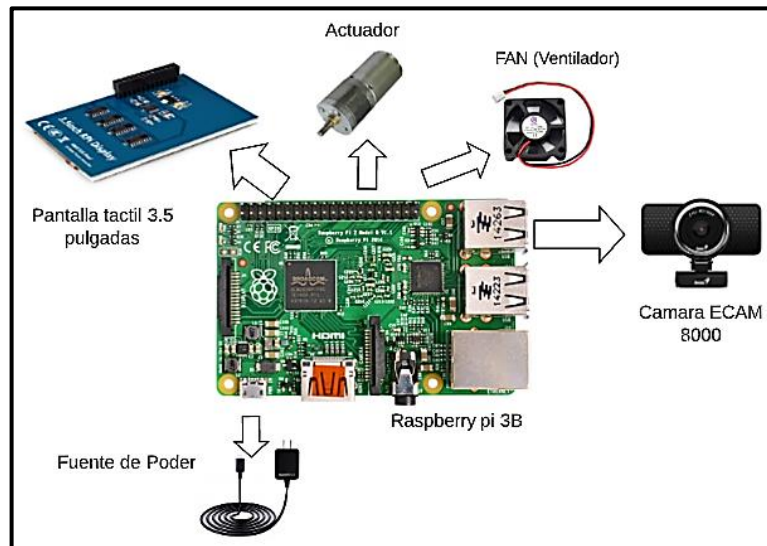
Figura 44. Pantalla Táctil 3.5 pulgadas.



Fuente: Autores. Hecho: 7/11/2019

En la figura 45, se ilustra la conexión necesaria de todos los dispositivos necesarios que necesita la Raspberry pi 3 B+ para el desarrollo del proyecto.

Figura 45. Esquema de conexión del proyecto.



Fuente: Autores. Hecho: 7/11/2019

## 11.2 INSTALACIÓN DEL SOFTWARE

Como se ha descrito anteriormente de la placa a utilizar es Raspberry Pi 3 B+, ya sabiendo sus características, es necesario saber la configuración de la misma, en primera instancia es necesario contar con una micro SD con un almacenamiento mayor a 8 GB que es el requerimiento mínimo para poder trabajar sobre esta, en este caso y para este proyecto, se utiliza una micro SD de 32 GB, para empezar a desarrollar sobre esta placa, se tiene que instalar el sistema operativo llamado Raspbian que viene con programas de educación ya preinstalados y de uso general, como lo es Python, Java, Scratch, entre otros.

Raspbian es una distribución de Linux basada en el sistema operativo Debian Buster, como pertenece a Linux quiere decir que su uso para educación o comercial es gratuito, la versión que se utilizó fue Raspbian Buster con escritorio, esto para tener una mejor experiencia con la interfaz de escritorio que siempre se maneja en cualquier S.O.

Lo primero que se debe hacer es descargar la imagen de Raspbian y posteriormente descomprimirla ya que descarga en formato comprimido, una vez teniendo la imagen descomprimida, se utiliza balenaEtcher que es una herramienta que escribe sobre tarjetas SD los archivos .iso que son las imágenes de los sistemas operativos o los .zip que son los archivos comprimidos. BalenaEtcher tiene un pequeño paso a paso detallado para el proceso de escritura en la SD, que es insertar la SD al computador que se está utilizando, luego cargar la imagen del S.O y por último darle click en el botón iniciar donde procede a formatear la micro SD en formato Fat 32 y grabar el .iso que contiene a Raspbian.

Teniendo lista la micro SD sin ningún tipo de error, se inserta en la ranura de la raspberry especialmente diseñada para la tarjeta de almacenamiento, se conecta el cable USB a la placa y el cable VGA a un monitor para poder visualizar la interfaz de la instalación. En el momento que arranca la placa, muestra la interfaz para instalar el sistema operativo, donde se escoge la distribución del teclado a utilizar y empieza a instalar todas las herramientas de software necesarias para que funcione el sistema operativo, una vez finalizado este proceso, se reinicia la Raspberry Pi 3 B+ y se visualiza el escritorio con la barra de herramientas en la parte superior y ya está lista para ser utilizada como placa de desarrollo.

Teniendo en cuenta lo anterior y estando en el escritorio de la Raspberry Pi 3 B+, se procede a abrir la terminal ya sea en menú o con Ctrl + Alt + T, para instalar los paquetes necesarios como lo es OpenCV que es una librería bastante completa en cuanto al tratamiento de imágenes, reconocimiento de características faciales, algoritmos de comparación, entre otras, esto se hace por medio de comandos por eso es necesario abrir la terminal del sistema operativo, en la figura 46, se listan los comandos utilizados para esta configuración.

Figura 46. Comandos para instalar OpenCV.

```
1 sudo raspi-config
2 sudo apt-get update
3 sudo apt-get upgrade
4 sudo apt-get install build-essential cmake pkg-config python-dev libgtk2.0-dev libgtk2.0 zlib1g-dev libpng-dev libjpeg-dev libtiff-dev libjasper-dev libavcodec-dev swig unzip
5 sudo apt-get install python-numpy python-opencv
6 sudo apt-get install python-pip
7 sudo apt-get install python-dev
8 wget http://downloads.sourceforge.net/project/opencvlibrary/opencv-unix/3.2.0/opencv-3.2.0.zip
9 unzip opencv-3.2.0.zip
10 cd opencv-3.2.0
11 cmake -DCMAKE_BUILD_TYPE=RELEASE -DCMAKE_INSTALL_PREFIX=/usr/local -DBUILD_PERF_TESTS=OFF -DBUILD_opencv_gpu=OFF -DBUILD_opencv_ocl=OFF -DWITH_V4L=ON -D
12 make
13 sudo make install
```

Fuente: Autores.

En la línea 1 de la figura 46, es para ingresar a la configuración de la Raspberry Pi 3 B+ y allí seleccionar la opción de expansión del sistema de archivos de la micro SD. La línea 2, se utiliza para obtener y descargar las actualizaciones que hasta el momento tiene Linux para Raspbian, para instalarlas y para actualizarlas se utiliza la línea 3, la 4<sup>ta</sup> línea, es donde se obtienen los paquetes Build-essential, estos principalmente son para la creación de paquetes o de scripts dentro de Raspbian, el 5<sup>to</sup> comando, obtiene e instala la librería numpy que es necesaria para el manejo de matrices y vectores en el procesamiento de imágenes por medio de la visión computacional que se realizará, En la línea 6, obtiene e instala el sistema de gestión de paquetes para administrar el entorno de programación que es Python, la línea 7, instala los archivos de encabezado que necesita cada librería en Python para utilizar archivos como .XML y no tener errores en la compilación.

La línea 8, descarga de esa dirección web el paquete comprimido de OpenCV 3.2.0 y luego descomprimirlo que se hace con el comando de la línea 9, en el comando de la línea 10, accede a la carpeta donde fue descomprimido el OpenCV y luego lo instala con la línea de comandos 11, y por último los comandos de las líneas 12 y 13, compilan el script de OpenCV para finalizar la instalación. La instalación se comprueba nuevamente ingresando a la terminal y digitando los comandos de la figura 47,

Figura 47. Comprobar la instalación de OpenCV.

```
1 python
2 >>import cv2
3 >>cv2.__version__
```

Fuente: Autores.

### 11.3 DETECCIÓN DEL ROSTRO Y CAPTURA

Ya instaladas las herramientas necesarias en la Raspberry pi 3 B+ se procede a diseñar el algoritmo, donde es necesario de dos scripts para poder realizar el reconocimiento facial, del primero se hablará en este subcapítulo y en el siguiente.



Lo primero que se debe entender es el cómo se realiza la captura del rostro que es lo que más importa para este proyecto. Teniendo en cuenta que OpenCV ya se instaló y sabiendo que esta biblioteca trata las imágenes y sus características, se debe hablar del archivo en cascada 'haarcascade\_frontalface\_alt.xml' declarado en la figura 48 del código,

Figura 48. Archivo cascada.

```
11 | fn_haar = 'haarcascade_frontalface_alt.xml'
```

Fuente: Autores.

este tiene una gran importancia en todo el proyecto, debido a que es el encargado de obtener la características de una persona en cuanto a rasgos faciales como el mismo archivo lo dice, contiene una base de datos de la parte frontal de la cara de miles de personas y previamente ya fue entrenado con todas estas fotos, lo que realiza es un algoritmo de comparación entre rasgos faciales y así determina los ojos, la boca, la nariz, las cejas y cada característica facial que puede llegar a tener una persona, de esta manera el entrenamiento que realiza es bastante completo, permitiendo una mayor eficacia en la comparación de características faciales.

En cuanto a la captura del rostro de cada foto tomada al usuario, se realiza por medio de la cámara ECam 8000, que se invoca por medio de programación como se evidencia en la figura 49.

Figura 49. Declaración de cámara.

```
21 | webcam = cv2.VideoCapture(0)
```

Fuente: Autores.

luego el algoritmo imprime el número (150) de fotos que le tomará al usuario para poder guardarlas en la base de datos, que en este caso es un fichero que se encuentra en el escritorio de la Raspberry Pi 3 B+ llamado 'Dataset', esta cantidad de fotos se declara en la siguiente línea de código de la figura 50.

Figura 50. Cantidad de fotos tomadas por persona.

```
22 | NumeroFotos =150
```

Fuente: Autores.

Una vez el algoritmo recibe la cantidad de fotos que debe tomar la cámara, abre la interfaz de la cámara permitiendo al usuario ver la cara de sí mismo y rodeándolo un recuadro de color verde que indica que se está reconociendo un rostro, es aquí donde actúa la línea de código 11 de la figura 48. Una vez terminado las capturas del rostro el algoritmo da por finalizado el proceso de la cámara y la apaga, y

pregunta, si las fotos tomadas desean ser entrenadas mediante el tratamiento de imágenes que OpenCV ofrece como herramienta, esto se visualiza en la figura 51.

Figura 51. Entrenamiento de modelo.

```
91 | etiqueta1=Label(ventana1,text='¿Desea entrenar el modelo? S/N')
```

Fuente: Autores.

Este entrenamiento se debe realizar solamente cuando el registro de usuarios al sistema haya finalizado de lo contrario no se debe realizar. Se debe tener en cuenta que el entrenamiento puede tardar ciertos minutos por la cantidad de imágenes que debe entrenar, es decir a más personas registras, más fotos, y a más fotos almacenadas, más tiempo dura el entrenamiento del algoritmo con el Dataset. Lo anterior se almacena en un archivo llamada 'Entrenamiento.XML', donde lo guarda en la carpeta principal donde se encuentran los algoritmos y el Dataset, 'ReconocimientoFacialTesis', una vez finalizado el entrenamiento guarda el archivo y muestra un mensaje de advertencia, 'Entrenamiento finalizado' y en la consola imprime 'programa finalizado', como se evidencia en la línea de código 80 y 81 respectivamente de la figura 52.

Figura 52. Entrenamiento y programa finalizado.

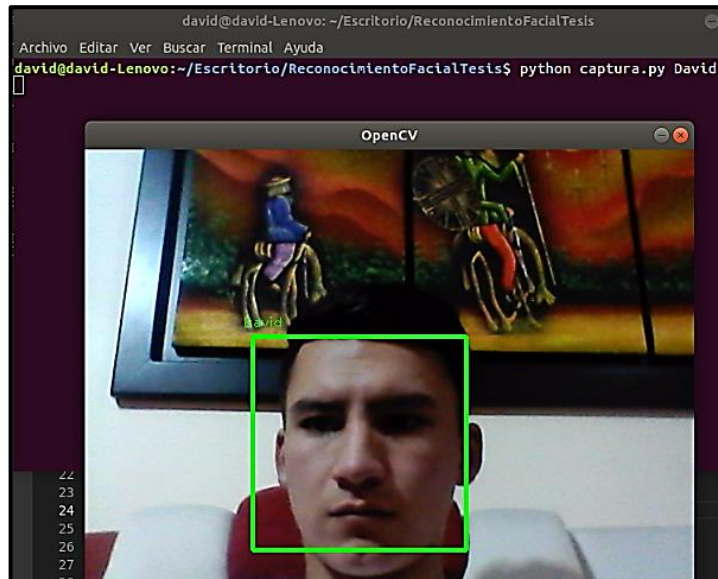
```
80 | messagebox.showwarning("Warning" ,"Entrenamiento finalizado")  
81 | print('Programa finalizado')
```

Fuente: Autores.

En el script de captura se ejecuta directamente desde la terminal, para lo cual es necesario poner al principio el programa al que hace referencia este para poder ejecutarlo, en este caso es Python.

Como siguiente paso se abre la interfaz de la cámara y de forma inmediata empieza a reconocer el rostro que está en la figura 53, y lo encierra en un recuadro de color verde para poder identificarlo y posteriormente entrenarlo.

Figura 53. Reconocimiento de rostro.



Fuente: Autores.

Una vez las 150 fotos tomadas del rostro, el algoritmo imprime por pantalla que se están creando las lista de imágenes y la lista de nombre correspondiente, de la misma forma crea la matriz de estas dos listas descritas, esto lo hace por medio de Numpy, posteriormente pregunta, si las muestras tomadas desean ser entrenadas, cabe recordar que el entrenamiento solo se hace cuando se acabe el registro de los usuarios, en la figura 54 se evidencia que empieza a entrenar el algoritmo, mientras que en la figura 55 muestra que no se deseó entrenar el algoritmo.

Figura 54. Condicional si se desea entrenar el algoritmo o no.

```
david@david-Lenovo: ~/Escritorio/ReconocimientoFacialTesis
Archivo Editar Ver Buscar Terminal Ayuda
david@david-Lenovo:~/Escritorio/ReconocimientoFacialTesis$ python captura.py David
Fotografias terminadas
Creando una lista de imagenes y de nombres correspondientes
Creando una matriz Numpy de las dos listas anteriores
Desea entrenar el modelo? s/n
1
Comenzando el entrenamiento
```

Fuente: Autores.

Figura 55. Condicional si se desea entrenar el algoritmo o no.

```
david@david-Lenovo: ~/Escritorio/ReconocimientoFacialTesis
Archivo Editar Ver Buscar Terminal Ayuda
david@david-Lenovo:~/Escritorio/ReconocimientoFacialTesis$ python captura.py David
Fotografías terminadas
Creando una lista de imágenes y de nombres correspondientes
Creando una matriz Numpy de las dos listas anteriores
Desea entrenar el modelo? s/n
0
Programa finalizado
david@david-Lenovo:~/Escritorio/ReconocimientoFacialTesis$
```

Fuente: Autores.

## 11.4 MANIPULACIÓN DE LA IMAGEN

En el subcapítulo anterior se describe la captura y la detección de rostro de la persona que está al frente de la cámara, más no se describe el proceso que realiza el algoritmo para tratar cada foto tomada.

El tratamiento de la imagen empieza con la siguiente línea de programación de la figura 56, hace que la imagen tomada tenga un tamaño de 112 Píxeles (px) de ancho y 92 px de alto, esto lo hace para que la imagen captada como rostro no sea mayor o menor a esta resolución ya que muchas veces la persona puede estar alejada o puede estar cerca de la cámara, esto evita que el tamaño varíe para una foto o para otra.

Figura 56. Tratamiento de la imagen.

```
19 (im_width, im_height) = (112, 92)
```

Fuente: Autores.

Una vez tomadas las 150 fotos con la cámara, el algoritmo ejecuta la línea 28 de la figura 57, donde permite que la foto tomada siempre esté de manera vertical, así la persona se haya inclinado un poco hacia la derecha o izquierda, también permite que cada foto que está tomando la cámara pase por esta línea y de este modo evitar errores al momento de realizar el entrenamiento y el reconocimiento.

Figura 57. Captura vertical.

```
28 im = cv2.flip(im, 1, 0)
```

Fuente: Autores.

En la línea 29 de la figura 58.

Figura 58. Escala de grises.

```
29 gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
```

Fuente: Autores.

Lo que hace es convertir la foto o el rostro capturado, a escala de grises, esto se debe a que el algoritmo de Eigen-faces necesita imágenes a blanco y negro para realizar la comparación de características faciales y así dar el resultado más óptimo de reconocimiento facial.

Entendiendo los subcapítulos 11.3 y 11.4, se ejecuta el programa de captura y reconocimiento de rostro de la siguiente manera, como se muestra en la línea 1 de la figura 59.

Figura 59. Comando para ejecutar captura.py.

```
1 Python captura.py Nombre_de_la_persona
```

Fuente: Autores.

Este nombre de la persona o usuario que se registra junto al momento de ejecutar el algoritmo de captura se realiza en la línea 14 y 15 de la figura 60, esta invoca la función que se evidencia en la figura 61.

Figura 60. Almacenamiento del nombre.

```
14 fn_name=nombre.get()  
15 print(nombre.get())
```

Fuente: Autores.

Figura 61. Función nombre.

```
106 hombre=StringVar()  
107 cajatexto=Entry(ventana, textvariable=nombre)  
108 cajatexto.place(x=100,y=20)
```

Fuente: Autores.

Donde lo almacena en un arreglo y posteriormente nombra la carpeta con el nombre de la persona que se registró, si no se introduce el nombre de la persona nueva a registrar, arrojará un error de sintaxis ya que necesita de este nombre para la captura del rostro y para el reconocimiento facial.

## 11.5 EXTRACCIÓN DE CARACTERÍSTICAS Y ALGORITMO DE RECONOCIMIENTO

La extracción de características principalmente la realiza el algoritmo ya descrito en el subcapítulo 11.3, teniendo en cuenta estas líneas de código dentro del algoritmo, se entiende que el algoritmo de reconocimiento facial está asociado al algoritmo de captura de imagen, permitiéndolo cargar dentro de este para que así compile el dataset almacenado en la base de datos y ejecute el algoritmo propio de reconocimiento, realizando la comparación necesaria para detectar la persona correcta.

El primer paso que realiza el algoritmo es la creación y la carga del método de reconocimiento facial llamado Eigen-faces, a continuación, en la figura 62 se muestra un fragmento del código donde se ven los llamados de variables, las declaraciones y sus funciones que realiza para completar el reconocimiento es su primera parte, de la línea 12 hasta la línea 23 de la figura 62, se crea una lista de imágenes y la lista correspondiente a cada nombre, teniendo en cuenta las imágenes cargadas del algoritmo llamado 'captura.py', la línea 24, se encarga de crear una matriz de imágenes también llamada Numpy, de las dos listas anteriormente creadas y declaradas, de esta forma crea y entrena un modelo a partir de las imágenes captadas en las listas y en la matriz, llevándolas al archivo 'Entrenamiento.XML', como se ve en las líneas 25 y 26.

Figura 62. Primera parte de reconocimiento.

```
12 (images, lables, names, id) = ([], [], {}, 0)
13 for (subdirs, dirs, files) in os.walk(fn_dir):
14     for subdir in dirs:
15         names[id] = subdir
16         subjectpath = os.path.join(fn_dir, subdir)
17         for filename in os.listdir(subjectpath):
18             path = subjectpath + '/' + filename
19             lable = id
20             images.append(cv2.imread(path, 0))
21             lables.append(int(lable))
22         id += 1
23 (im_width, im_height) = (112, 92)
24 (images, lables) = [numpy.array(lis) for lis in [images, lables]]
25 model1 = cv2.face.createEigenFaceRecognizer()
26 model1.load("Entrenador.yml")
```

Fuente: Autores.

Como siguiente paso para dar continuación a la ejecución del algoritmo, se compila la siguiente línea de código (ver figura 63), que es la que permite la predicción de la cara a reconocer, con el modelo ya creado, cargado y entrenado de las líneas 25 y 26 de la figura 62

Figura 63. Predicción.

```
59 prediction = model1.predict(face_resize)
```

Fuente: Autores.

Para concluir la ejecución del algoritmo, se compilan las líneas de código que en la figura 64 se enumeran.

Figura 64. Segunda parte de reconocimiento.

```
72 if cara == "Nombre1":
73     cv2.putText(frame, 'David', (x-10, y-10), cv2.FONT_HERSHEY_PLAIN, 1, (0, 255, 0))
74     cv2.imshow('OpenCV', frame)
75     cNombre1 = cNombre1 + 1
76 if cDavid == Seguridad:
77     print('Se ha detectado a:')
78     print(cara)
79     webbrowser.open_new(url)
80     GPIO.setmode(GPIO.BOARD)
81     GPIO.setup(40, GPIO.OUT)
82     GPIO.output(40, True)
83     time.sleep(7)
84     GPIO.output(40, False)
85     print("Si desea analizar otra cara digite S")
86     rep = int(input('En caso contrario digite 0\n'))
87 if rep == 0:
88     os.kill(os.getppid(), signal.SIGHUP)
89 else:
90     cNombre1 = 0
```

Fuente: Autores.

Estas líneas son las más importantes respecto a la comparación, ya que son las encargadas de decidir si la persona que la cámara está viendo coincide o no con la persona registrada en la base de datos. En la línea 72, la variable cara se iguala al nombre de la persona uno, si esto es correcto, por medio de OpenCV, envía a la ventana emergente con el rostro detectado el nombre de la persona 1, de lo contrario no lo hará, como se describe en la línea 73, la línea 74, se encarga de mostrar este recuadro ya descrito anteriormente, compilando la línea 75, se realizó una comparación, añadiendo una variable de seguridad que es la que permite que tanto tiempo se deba analizar a una persona para poder arrojar un resultado, por esta razón la comparación que realiza es que sea igual a la variable cNombre1, que es la variable que capta el valor numérico del rostro y lo iguala a la variable seguridad.

Cabe añadir que a mayor seguridad, mayor es el tiempo de compilación y de mostrar el resultado de reconocimiento facial, posteriormente, en las líneas 77 y 78 imprime por pantalla la persona que fue detectada o reconocida según la comparación ya realizada y por último de la línea 79 hasta la línea 90, envía la señal a los puertos GPIO para dar acceso o no, por otro lado, el algoritmo también pregunta si se desea analizar otro rostro, donde si el resultado es si, nuevamente se repite el ciclo del algoritmo desde la línea 72, y así hasta reconocer a las 4 personas, para lo cual está hecho el sistema.

## 11.6 INTERFAZ GRÁFICA

Esta es la parte grafica que vera el usuario en el proyecto y es la que tendrá comunicación entre la persona usuario y el sistema. Esta parte es vital para que el usuario maneje las varias opciones que tiene el programa de una forma cómoda y comprensible.

**11.6.1 Creación de la interfaz gráfica.** En este apartado se realizó la interfaz gráfica que se usó para el sistema; y a continuación se describen los comandos utilizados para esto. Cabe aclarar que esta interfaz fue realizada a través de funciones internas y librerías como se muestra en la figura 65 para que tuviera una mayor organización y compresión del código, por esta razón se describirán las funciones por partes. Si se desea ver el código completo este estará ubicado en la parte de Anexos C.

Figura 65. Librerías.

```
1  import RPi.GPIO as GPIO
2  import webbrowser as wb
3  import tkinter as tk
4  import os
5  import time
6  from io import open
7  from tkinter import messagebox
8  from tkinter import ttk
9  from tkinter import *
```

Fuente: Autores.

Como primera parte se tuvieron que agregar algunas librerías que se utilizaron durante el proyecto como la librería de tkinter para interfaces gráficas, RPI para utilizar los puertos GPIO de la Raspberry Pi 3 B+, la Librería messagebox para agregar cuadros de alerta.



- **Función Principal**

La función principal que se evidencia en la figura 66, contiene la interfaz gráfica de la página principal y esta contiene desde el tamaño, diseño, color de fondo, imágenes insertadas hasta la ubicación y la creación de los botones, cabe aclarar que en la creación de los botones cuando se oprimen estos tienen integrados las funciones donde se deben dirigir.

Figura 66. Función principal de Interfaz.

```
95 pri =tk.Tk()
96 pri.geometry('2000x2000')
97 pri.configure(background= 'black')
98 pri.title("Reconocimiento facial")
99 e3=tk.Label(pri,text="Bienvenido",bg="black",fg="white")
100 e3.pack(padx=5,pady=5,ipadx=5,ipady=5,fill=tk.X)
101 imagen=PhotoImage(file="reco.png")
102 fondo=Label(pri,image=imagen).place(x=1,y=40)
103 #Reco= os.system('python3 reconocimiento.py')
104 def reconocimiento():
105     os.system("python3 reconocimiento.py")
106 e4=tk.Button(pri,text="Entrar por reconocimiento facial",bg="black",fg="white",command=reconocimiento)
107 e4.place(x=160, y=610, width=220, height=70)
108
109 boton7=tk.Button(pri,text="Entrar por clave usuario",bg="black",fg="white", command= clave)
110 boton7.place(x=160, y=530, width=220, height=70)
111
112 boton4=tk.Button(pri,text="Configuracion",bg="black",fg="white", command= admin)
113 boton4.place(x=160, y=450, width=220, height=70)
```

Fuente: Autores.

Por ejemplo, el botón e4 abre el archivo de reconocimiento facial el cual enciende la cámara y empieza a verificar el rostro de la persona

- **Función Validar**

Esta función (ver figura 67) permite validar a las personas que ingresan a la configuración del sistema por medio de un usuario o contraseña, esta será validada con unos parámetros guardados en código. De igual manera esta función contiene el diseño de la interfaz Login.

Figura 67. Función validar.

```
31 def validar():
```

Fuente: Autores.

- **Función Validar2**

Esta función (ver figura 68) valida la entrada a la vivienda por medio de un usuario y una contraseña, también esta especifica la activación de un puerto GPIO de la Raspberry Pi 3 B+ cuando el usuario y la contraseña es correcta.

Figura 68. Función validar 2.

```
56 | def validar2():
```

Fuente: Autores.

- **Función abrirventana2**

Esta función (véase figura 69) es donde se encuentra ubicada la interfaz de configuración para esto primero se tiene que entrar a la interfaz de validación y llegar los campos vacíos con el usuario y la contraseña correctos. Esta contiene el diseño de la interfaz y la configuración de los botones existentes como “Editar y eliminar”, “Agregar usuario”. Dentro de esta función se encuentran dos funciones más.

Figura 69. Función abrir ventana 2.

```
12 | def abrirventana2():
```

Fuente: Autores.

- **Función Eliminar**

Esta función (véase figura 70) redirecciona a la ubicación donde se encuentra la base de datos de los usuarios registrados.

Figura 70. Función eliminar.

```
20 | def eliminar():  
21 |     wb.open_new('/home/pi/Desktop/ReconocimientoFacialTesis/caras')
```

Fuente: Autores.

- **Función Agregar**

Esta función (véase figura 71) direcciona y activa un archivo .py el cual agrega el nombre de una persona y le toma una serie de fotos para guardarla en una base de datos.

Figura 71. Función agregar/captura.

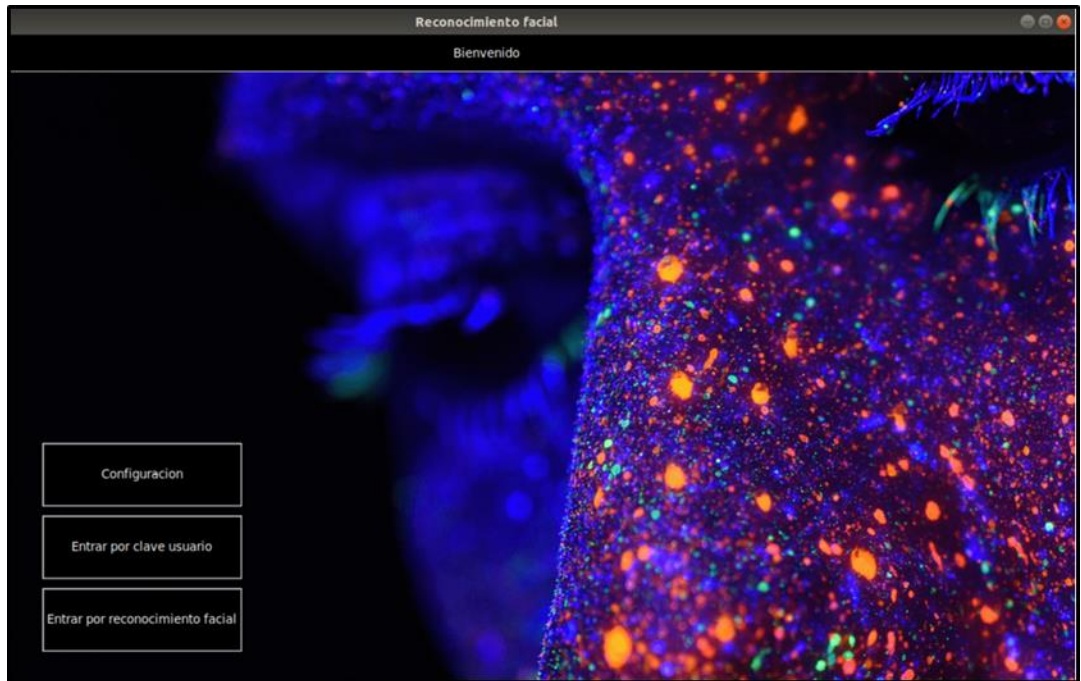
```
20  ▾ | def captura():
```

Fuente: Autores.

**11.6.2 Guía de usuario de la interfaz.** Esta interfaz gráfica está compuesta por una página principal, Login, Configuración, Editar y eliminar, Agregar.

La página principal llamada “Reconocimiento facial” es la que se visualiza como inicio del sistema y es la que contiene todas las opciones generales dentro del programa como se evidencia en la figura 72, tiene tres opciones.

Figura 72. Interfaz gráfica: Reconocimiento facial.



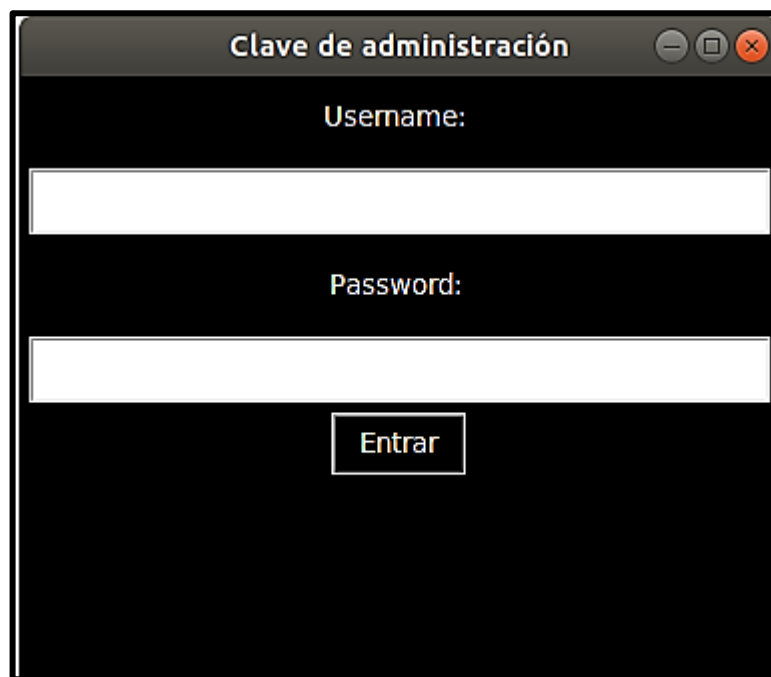
Fuente: Autores.

1. Entrar por reconocimiento facial: Esta permite activar el sistema que se compone del algoritmo y la cámara para que empiecen su funcionamiento de reconocimiento, el sistema cuando reconoce a una persona de inmediato activa un puerto GPIO que arroja 3.3 voltios, este mediante un circuito de control activa un interruptor que prende un bombillo de 110voltios. Si, por el contrario, el sistema no ha reconocido a ninguna persona este se detendrá y se tendrá que ir al menú principal.

2. Configuración: Esta opción despliega una Login de usuario y contraseña que identifica a un usuario como administrador o no, esta opción es para que un administrador pueda borrar, modificar o ingresar un usuario nuevo.
3. Entrar por clave usuario: Este botón permite activar el Login de usuario para que active el mecanismo de apertura que en este caso es una bombilla de 110 voltios.

El Login de clave de administración es una pantalla que contiene dos espacios como se evidencia en la figura 73, y esta permite ingresar a la configuración del sistema.

Figura 73. Interfaz gráfica: Clave de administración.



Fuente: Autores.

En el primer espacio hay un cuadro para ingresar el nombre del usuario que quiere entrar, y en el segundo espacio se encuentra el cuadro de contraseña, si estos dos son correctos, abrirá la pestaña de administrador.

El Login de Clave de ingreso es una pantalla que contiene dos espacios como se evidencia en la figura 74, y esta permite si los valores son correctos el ingreso al usuario por medio de la activación de un bombillo de 110 voltios.

Figura 74. Interfaz gráfica: Clave de ingreso.

A screenshot of a graphical user interface window titled "Clave de ingreso". The window has a dark background and a light-colored title bar with standard window controls (minimize, maximize, close). Below the title bar, the text "Username:" is displayed above a white rectangular input field. Below this, the text "Password:" is displayed above another white rectangular input field. At the bottom of the window, there is a button with the text "Validar password".

Fuente: Autores.

La ventana de configuración es la encargada de mostrar las configuraciones en cuanto a los usuarios registrados en el sistema, esta interfaz de configuración contiene 3 botones como se evidencia en la figura 75. Estos botones se componen de:

1. Modificar: esta opción desplegará la ubicación de la base de datos de cada persona registrada en el sistema, acá se podrán modificar nombres de los usuarios del sistema.
2. Agregar usuario: Esta opción desplegará una ventana que en primera parte contiene la petición de un nombre nuevo para guardar al sistema. Después de esto se encenderá la cámara para agregar a la base de datos las imágenes del usuario que se está registrando.

3. Eliminar: este botón redirecciona a la ubicación de la base de datos de cada persona registrada en el sistema, acá se podrán eliminar usuarios del sistema si se desea.

Figura 75. Interfaz gráfica: Administrador.



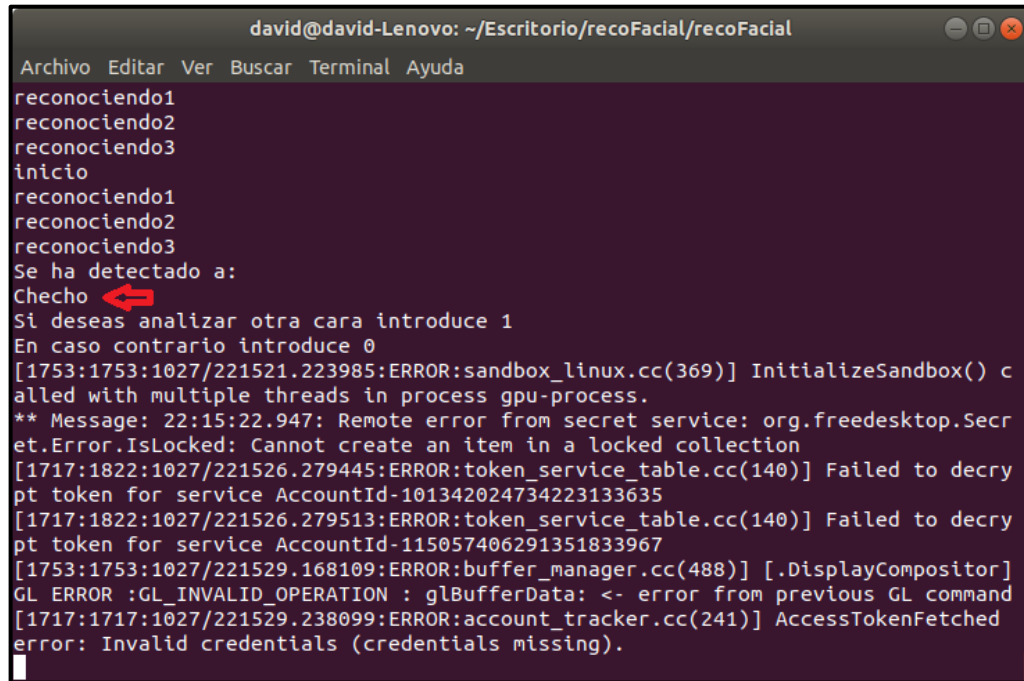
Fuente: Autores.

## 11.7 PRUEBAS DE EFICACIA

En el momento que se inicializa el algoritmo de reconocimiento facial, se ejecuta en la terminal de la misma manera que se ejecutó la primera parte, 'python reconocimiento.py', de esta forma se empieza a ejecutar el algoritmo.

Posteriormente el algoritmo empieza a hacer el reconocimiento facial, pasando por la detección de rostro y el análisis de características, imprimiendo por pantalla a la persona que se reconocer, en este caso es la persona llamada Checho la cual se puede evidenciar en la figura 76 y la figura 77.

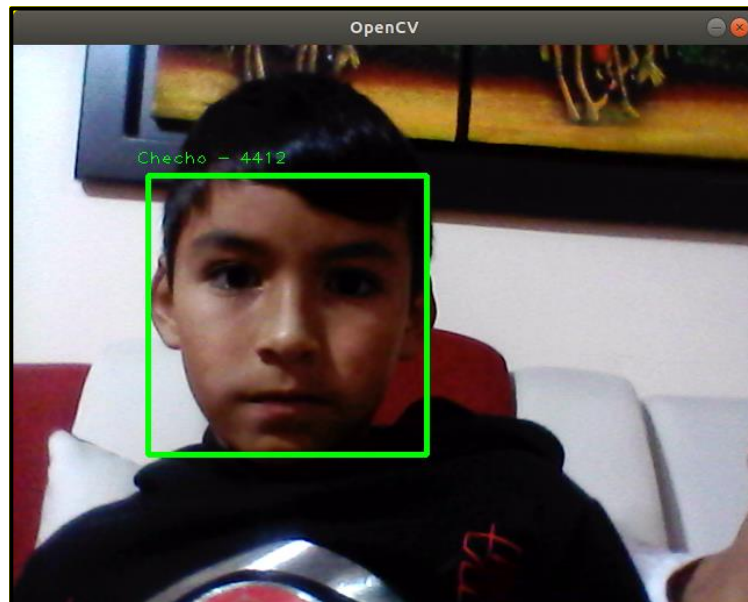
Figura 76. Reconocimiento facial de Checho (I).



```
david@david-Lenovo: ~/Escritorio/recoFacial/recoFacial
Archivo Editar Ver Buscar Terminal Ayuda
reconociendo1
reconociendo2
reconociendo3
inicio
reconociendo1
reconociendo2
reconociendo3
Se ha detectado a:
Checho ←
Si deseas analizar otra cara introduce 1
En caso contrario introduce 0
[1753:1753:1027/221521.223985:ERROR:sandbox_linux.cc(369)] InitializeSandbox() called with multiple threads in process gpu-process.
** Message: 22:15:22.947: Remote error from secret service: org.freedesktop.Secret.Error.IsLocked: Cannot create an item in a locked collection
[1717:1822:1027/221526.279445:ERROR:token_service_table.cc(140)] Failed to decrypt token for service AccountId-101342024734223133635
[1717:1822:1027/221526.279513:ERROR:token_service_table.cc(140)] Failed to decrypt token for service AccountId-115057406291351833967
[1753:1753:1027/221529.168109:ERROR:buffer_manager.cc(488)] [.DisplayCompositor] GL ERROR :GL_INVALID_OPERATION : glBufferData: <- error from previous GL command
[1717:1717:1027/221529.238099:ERROR:account_tracker.cc(241)] AccessTokenFetched error: Invalid credentials (credentials missing).
```

Fuente: Autores.

Figura 77. Reconocimiento facial de Checho (II).



Fuente: Autores.

La segunda prueba de reconocimiento facial se realiza con uno de los autores del trabajo de grado, en este caso David, para este reconocimiento se digita la opción 1 del algoritmo en la parte que pregunta que, si se desea analizar otra persona, en la figura 78 y en la figura 79, se muestra el reconocimiento facial completo.

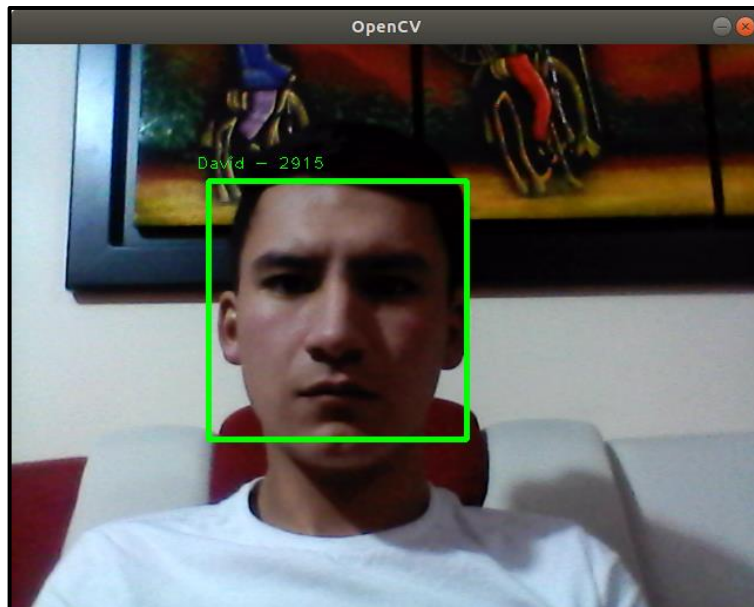
Figura 78. Reconocimiento facial de David (I).

```
david@david-Lenovo: ~/Escritorio/recoFacial/recoFacial
Archivo Editar Ver Buscar Terminal Ayuda
inicio
reconociendo1
reconociendo2
reconociendo3
inicio
reconociendo1
reconociendo2
reconociendo3
inicio
reconociendo1
reconociendo2
reconociendo3
inicio
reconociendo1
reconociendo2
reconociendo3
Se ha detectado a:
David
Si deseas analizar otra cara introduce 1
En caso contrario introduce 0
[7558:7558:1027/220415.988136:ERROR:sandbox_linux.cc(369)] InitializeSandbox() called with multiple threads in process gpu-process.
Abriendo en una sesión existente del navegador
```

Fuente: Autores



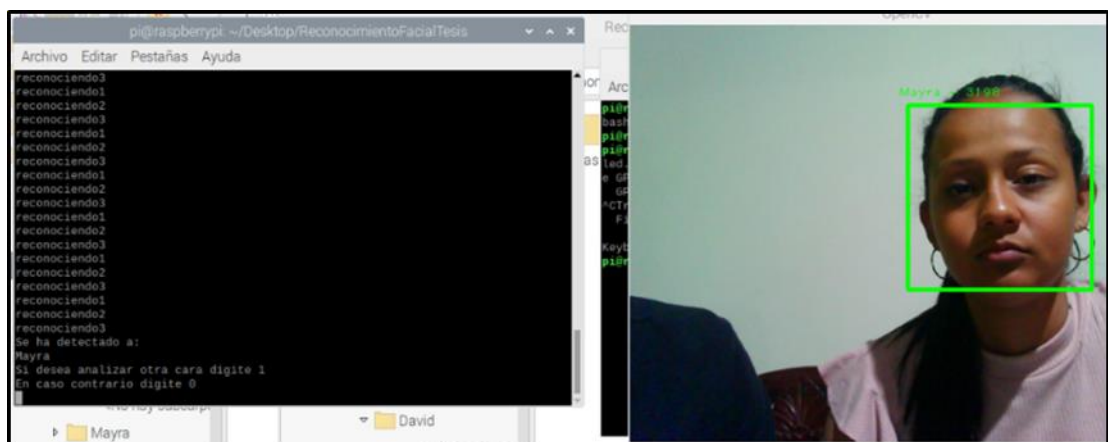
Figura 79. Reconocimiento facial de David (II).



Fuente: Autores

La tercera prueba de reconocimiento facial se realiza con una mujer llamada Mayra, la cual tiene aretes como accesorio facial, esto permite que el algoritmo se exija mucho más para realizar el reconocimiento, en la figura 80, se evidencia la fotografía con la etiqueta de ella y en la parte izquierda el nombre de Mayra en la terminal.

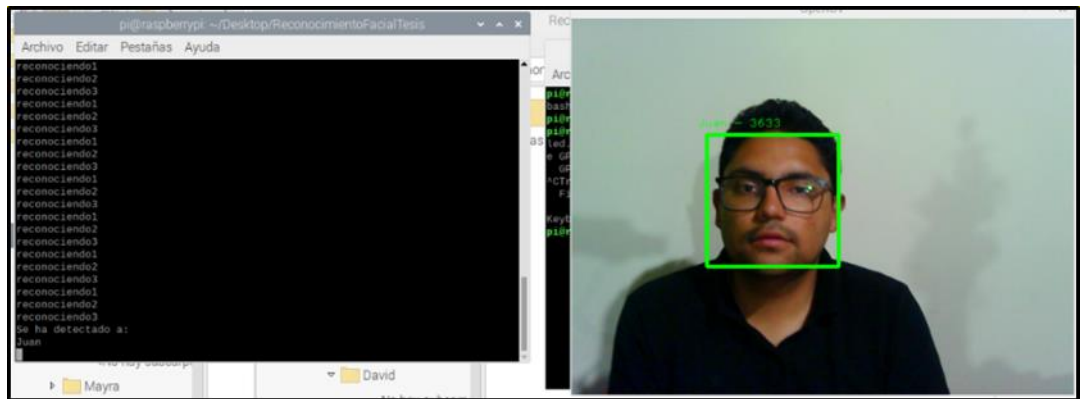
Figura 80. Reconocimiento facial de Mayra.



Fuente: Autores.

La cuarta y última prueba del reconocimiento facial se realiza con otro de los autores del proyecto de grado, llamado Juan, él en este caso tiene gafas ya que siempre suele estar con gafas, en la figura 81, a la derecha se logra ver a Juan con la etiqueta correspondiente a él, y en la parte izquierda de la figura, se evidencia el nombre de él en la terminal como resultado del algoritmo.

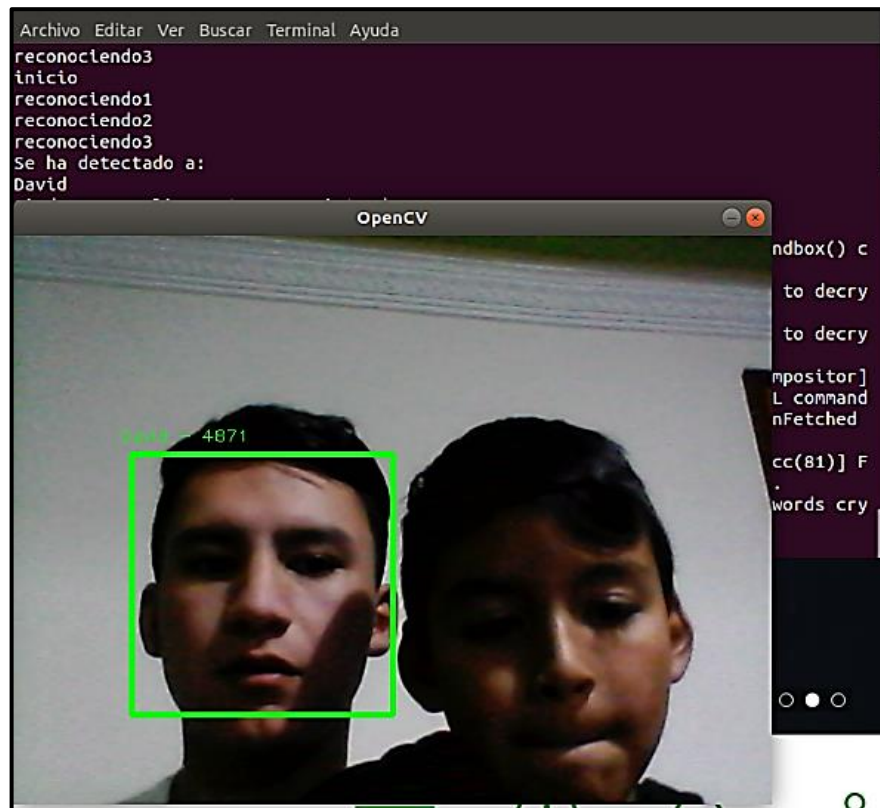
Figura 81. Reconocimiento facial de Juan.



Fuente: Autores.

Por otro lado, y sin dejar atrás la comparación de los algoritmos, se tiene en cuenta un gran factor el cual es de gran importancia, al momento de instalar la cámara en la puerta es claro que habrá más personas cerca al rostro el cual se quiere reconocer, por esta razón se hizo una prueba con respecto a la luminosidad y al acercamiento. El reconocimiento facial siempre se lo hará a la persona más cercana y que la cámara determine que es la mejor imagen o rostro para analizar y procederlo a analizar para luego reconocerlo, en la figura 82, se visualiza la prueba como se ejecutó de una manera más clara y explicada por sí misma.

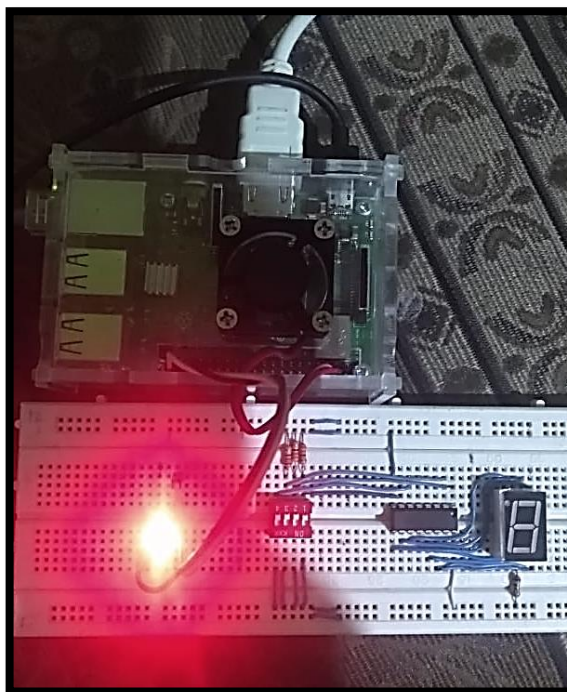
Figura 82. Reconocimiento facial de David.



Fuente: Autores.

Una vez realizado el reconocimiento facial para las personas que sean necesarias, esto pasará a activar un LED el cual se evidencia en la figura 83, activando el pin 40 o GPIO 21 de las Raspberry Pi 3 B+, esto se realiza mediante código que se dejará en anexos. Cabe aclarar que solo hace la activación del LED por lo que lo demás que hay en la protoboard no tendrá importancia para la prueba ya que no corresponde a esta. Finalmente se evidencia el prototipo final en la figura 84, con lo cual se probó el sistema con éxito.

Figura 83. Activación de LED por medio de reconocimiento facial.



Fuente: Autores.

Figura 84. Prototipo final.



Fuente: Autores.

**11.7.1 Reconocimiento facial bajo características típicas de acceso.** En este apartado se realizaron pruebas que miden la eficiencia del algoritmo con condiciones típicas de acceso tales como: acceso en diferentes franjas horarias, el uso de accesorios en el rostro, el ángulo de inclinación de la cámara, gestos comunes, y características variantes; cabe recalcar que algunas de las fotos usadas en estas pruebas se localizan en el Anexo A.

Para estas pruebas se tomaron 4 personas, a las cuales se les tomaron un set de aproximadamente 100 fotos por persona, estas cuatro personas lo componen, una mujer, tres hombres que dentro de ellos está incluido un niño, se tuvieron en cuenta unos tiempos aceptables de reconocimiento facial como se muestra en la tabla 16 con los cuales se dedujo el porcentaje y se clasificaron los mismo.

Tabla 16. Clasificación de porcentajes y tiempos para el reconocimiento facial.

<b>CLASIFICACIÓN DE RECONOCIMIENTO FACIAL</b>	
Pocentaje (%)	Tiempo (s)
95 a 100	0 a 3
90 a 95	4 a 7
80 a 90	8 a 11
70 a 80	12 a 16
50 a 70	Más de 16
0 a 50	Más de 21

Fuente: Autores.

A continuación, se describirán las tablas que conforman las condiciones típicas para cada usuario analizado.

En la tabla 17, se realizan las pruebas de iluminación donde la luz natural es la que se produce durante el día y la luz artificial es la que está presente por un dispositivo lumínico activado en las horas de la noche o en horas en que esté muy oscuro el día. Se tomaron las pruebas y se clasificaron según cada persona como se evidencia en la tabla 18.

Tabla 17. Pruebas de reconocimiento facial bajo condición lumínica.

<b>PRUEBAS DE ILUMINACIÓN</b>		
	<b>PORCENTAJE DE RECONOCIMIENTO (%)</b>	
	Luz natural	Luz Artificial
Mayra	99.96	98.04
Checho	98.03	92.8
Juan	99.03	95.60
David	99.02	97.10

Fuente: Autores.

Tabla 18. Clasificación de porcentajes y muestras para tabla de iluminación.

<b>Clasificación</b>			
		Muestras (Fotos)	Porcentaje (%)
Mayra	Luz natural	2 y 98	98 y 100
	Luz artificial	2 y 98	100 y 98
Checho	Luz natural	1 y 99	100 y 98
	Luz artificial	10 y 90	100 y 92
Juan	Luz natural	3 y 97	100 y 99
	Luz artificial	10, 20 y 70	100, 92 y 96
David	Luz natural	2 y 98	100 y 99
	Luz artificial	30, 30 y 40	98, 99 y 95

Fuente: Autores.

En el reconocimiento facial la luz juega una parte importante, por esta razón entre más claros estén los rasgos faciales de una persona el algoritmo lo reconocerá mejor, y esto es claro ejemplo de los resultados visualizados donde el reconocimiento en luz natural es más eficiente que el reconocimiento con luz artificial, aunque es muy poca la diferencia son datos que no se pueden despreciar.

Por esta razón, se hicieron pruebas con accesorios para evidenciar los porcentajes y la eficiencia del algoritmo con estas, estos se evidencian en la tabla 19, mientras que en la tabla 20 se logra ver el porcentaje que se obtuvo según el tiempo de respuesta para cada usuario.

Tabla 19. Pruebas de reconocimiento facial bajo condición de accesorios.

<b>PRUEBAS CON ACCESORIOS</b>				
	<b>PORCENTAJE DE RECONOCIMIENTO (%)</b>			
	Gafas	Gorra	Aretes	Pañoleta
Mayra	98.04	64.1	98.04	81.15
Checho	90.0	87.6	N/A	86.4
Juan	95.60	75.9	N/A	84.05
David	95.05	78.75	N/A	88.26

Fuente: Autores.

Tabla 20. Clasificación de porcentajes y muestras para tabla de accesorios.

<b>Clasificación</b>			
		Muestras (Fotos)	Porcentaje (%)
Mayra	Gafas	2 y 98	100 y 98
	Gorra	5 y 96	66 y 64
	Aretes	2 y 98	100 y 98
	Pañoleta	15 y 85	82 y 81
Checho	Gafas	2 y 98	100 y 98
	Gorra	20 y 80	90 y 87
	Aretes	N/A	N/A
	Pañoleta	20 y 80	88 y 86
Juan	Gafas	100	90
	Gorra	30 y 70	96 y 95%
	Aretes	N/A	N/A
	Pañoleta	5 y 95	85 y 84
David	Gafas	5 y 95	96 y 95
	Gorra	25 y 75	78 y 79
	Aretes	N/A	N/A
	Pañoleta	13 y 87	90 y 88

Fuente: Autores.

Por otro lado, es importante tener en cuenta en ángulo de inclinación que una cámara tiene para con el usuario, esto es porque este proyecto se basa en un sistema de seguridad para una vivienda por medio de reconocimiento facial, la cámara para todas las personas no estará al mismo ángulo, por eso fue necesario realizar estas pruebas y así identificar las falencias y las mejoras que tiene el algoritmo, esta información se puede observar en la tabla 21, con 0, 20, 30 y 45 grados para cada persona analizada, y en la tabla 22, se evidencian las muestras y sus respectivos porcentajes que se tuvieron en cuenta para la clasificación.

Tabla 21. Pruebas de reconocimiento facial bajo condición de ángulos de inclinación.

<b>PRUEBAS CON ANGULOS DE INCLINACIÓN</b>				
	<b>PORCENTAJE DE RECONOCIMIENTO (%)</b>			
	0°	20°	30°	45°
Mayra	98.04	82.36	77.6	69.6
Checho	92.8	87.91	81.64	77.15
Juan	95.6	90.21	84.5	75.08
David	97.1	95.4	93.6	98.1

Fuente: Autores.

Tabla 22. Clasificación de porcentajes y muestras para tabla de ángulos de inclinación.

<b>Clasificación</b>			
		Muestras (Fotos)	Porcentaje (%)
Mayra	0°	2 y 98	100 y 98
	20°	2 y 98	100 y 82%
	30°	20 y 80	80 y 77
	45°	5 y 95	81 y 69
Checho	0°	10 y 90	100 y 92
	20°	7 y 93	100 y 87
	30°	18 y 82	80 y 82
	45°	15 y 85	78 y 77
Juan	0°	10, 20 y 70	100, 92 y 96
	20°	11 y 89	100 y 89
	30°	10 y 90	89 y 84
	45°	8 y 92	76 y 75
David	0°	30, 30 y 40	98, 99 y 95
	20°	8 y 92	100 y 95
	30°	10 y 90	90 y 94
	45°	10 y 90	99 y 98

Fuente: Autores.

En la tabla 23, se realizaron pruebas del reconocimiento facial y el algoritmo, con gestos característicos del ser humano, como lo es la sonrisa, muecas, ojos cerrados, y la prueba más difícil es donde la persona tiene la cara de perfil, en esta prueba se evidenció que el algoritmo no reconoce a personas que están de lado, ya que no captura el rostro es esta la razón por la cual no hace el reconocimiento facial, en la tabla 24, se evidencian las 100 fotos tomas al usuario y su clasificación que tiene como porcentaje para cada característica facial o gesto.

Tabla 23. Pruebas de reconocimiento facial bajo condición de gestos.

<b>PRUEBAS CON GESTOS</b>				
	<b>PORCENTAJE DE RECONOCIMIENTO (%)</b>			
	Sonrisa	Ojos cerrados	Mueca	Cara de perfil
Mayra	97.3	94.48	94.9	0
Checho	97.6	95.5	97.51	0
Juan	98.1	97.06	98.1	0
David	98.16	94.3	92.32	0

Fuente: Autores.



Tabla 24. Clasificación de porcentajes y muestras para tabla de gestos.

<b>Clasificación</b>			
		Muestra (Fotos)	Porcentaje (%)
Mayra	Sonrisa	10 y 90	100 y 97
	Ojos cerrados	8 y 92	100 y 94
	Mueca	15 y 85	100 y 94
	Cara de perfil	100	0
Checho	Sonrisa	20 y 80	100 y 97
	Ojos cerrados	10 y 90	100 y 95
	Mueca	17 y 83	100 y 97
	Cara de perfil	100	0
Juan	Sonrisa	5 y 95	100 y 98
	Ojos cerrados	2 y 98	100 y 97
	Mueca	5 y 95	100 y 98
	Cara de perfil	100	0
David	Sonrisa	8 y 92	100 y 98
	Ojos cerrados	5 y 95	100 y 94
	Mueca	4 y 96	100 y 97
	Cara de perfil	100	0

Fuente: Autores.

Desde la tabla 16 hasta la tabla 24, se logran mostrar resultados con porcentajes óptimos, porque la mayoría de pruebas se realizaron con la cámara en frente, mientras que la tabla 25, las pruebas son características variantes, como es la rotación de la cara, quiere decir que la cara está hacia un lado pero mirando la cámara, otra variante como la traslación, que es taparse la mitad del rostro con algún objeto y la variante a escala, es alejarse la cámara lo máximo posible, en este caso se evidencia que la distancia máxima en que se reconoce a una persona es a 1.5 metros, si la persona está más alejada no la reconoce, por tal razón se hicieron pruebas a esta distancia. Los porcentajes de esta prueba y sus muestras se pueden ver en la tabla 26.

Tabla 25. Pruebas de reconocimiento facial bajo condición de características variantes.

<b>PRUEBAS CON CARACTERISTICAS VARIANTES</b>			
	PORCENTAJE DE RECONOCIMIENTO (%)		
	Rotación	Traslación	Escala
Mayra	11.0	0	82.36
Checho	15.0	0	99
Juan	12.0	0	72.08
David	13.0	0	84.22

Fuente: Autores.

Tabla 26. Clasificación de porcentajes y muestras para tabla características variantes.

<b>Clasificación</b>			
		Muestras (Fotos)	Porcentaje (%)
Mayra	Rotación	100	11
	Traslación	100	0
	Escala	2 y 98	100 y 82
Checho	Rotación	100	15
	Traslación	100	0
	Escala	100	50
Juan	Rotación	100	12
	Traslación	100	0
	Escala	8 y 92	73 y 72
David	Rotación	100	13
	Traslación	100	0
	Escala	11 y 89	86 y 84

Fuente: Autores.

## **12.RESULTADOS ESPERADOS**

Se espera que este proyecto desarrollado e implementado ayude en cierta forma a los ciudadanos a confrontar la inseguridad que se ve en la ciudad, implantando el sistema seguridad con reconocimiento facial el cual hará factible el acceso a las viviendas, dando un mejor control al usuario y automatización en el hogar.

Además, este proyecto realizado puede expandirse como parte de una investigación más exhaustiva para mitigar la inseguridad en la ciudad en cuanto hurtos a viviendas y pueda ser más eficiente en tareas caseras en el hogar como la interacción con los usuarios dentro del hogar, dado que es un sistema bastante útil, se puede utilizar junto a la cámara de la ciudad para reconocer personas buscadas por la justicia colombiana.

### 13. CONCLUSIONES

Al hacer la recopilación de información de las técnicas de reconocimiento facial se evidencia que muchas de ellas eran bastante viables para utilizarlas en este proyecto, sin embargo, se tomó la decisión de usar la técnica de reconocimiento facial Eigen-faces junto al PCA, debido a varias razones que la anteponen. Estas razones son por su baja complejidad computacional y su poca utilización de recursos de la imagen, lo hacen que tenga un tiempo de respuesta muy aceptable, y el reconocimiento sea de un 97% preciso. Además de ser uno de los algoritmos más conocidos y confiables por la comunidad investigadora, este puede acoplarse con otras técnicas para mejorar el entrenamiento de las imágenes de referencia.

Durante la definición de requerimientos tanto de las herramientas software, hardware y del algoritmo, todas ellas se basaron en el ambiente de trabajo en la que se implementó el sistema. por esta razón se tuvieron en cuenta características propias de una casa; Estas características pueden afectar el funcionamiento ideal si estas no se tienen en cuenta para la implementación de dicho sistema, ya que este podría tener fallas o inclusive hacer que el reconocimiento facial no sea un método seguro para el control de acceso, por esta razón los requerimientos que se expusieron en el capítulo 12 son características o condiciones que deben tener el sistema en general para mitigar los efectos de un ambiente no controlado como la luz natural, el color de piel de una persona, rasgos que varían con el tiempo, o inclusive la calidad de la cámara.

En la implementación del sistema se verifico la eficiencia del algoritmo Eigen faces haciendo pruebas con diferentes ítems, poses y condiciones de luz, además de esto, se hicieron pruebas con un niño, una mujer y dos jóvenes adultos, lo cual comprueba que el sistema no diferencia entre géneros. También al implementar el sistema se evidencio que este algoritmo se basa en la posición y el contorno de los ojos por esta razón cuando se hacen pruebas de traslación su porcentaje de reconocimiento es bastante bajo.

Los porcentajes de reconocimiento vistos en las pruebas de eficacia dependen mucho de las fotos de entrenamiento que se realicen, entre más fotos y más poses se hagan, será mejor el reconocimiento facial. En cuanto a los grados de inclinación de la cámara se obtuvieron resultados muy bajos de reconocimiento, debido a que, a la hora de la toma de muestras para el almacenamiento de las fotos, estas se tomaron en un solo ángulo de inclinación por este motivo es aconsejable que cuando ya esté instalada la cámara se realice el almacenamiento de muestras y se haga en el entrenamiento de las mismas, para obtener mejores resultados.

Este proyecto aunque desarrollado para el uso en viviendas, no está excluido de utilizarlo en otros lugares como fábricas o empresas, donde el sistema de seguridad

debe ser confiable, sin embargo para estos casos se deberían hacer estudios previos antes de implementar este sistema en otros lugares, ya que el sistema propuesto tiene características particulares como: el mínimo de personas que tiene el sistema, la base de datos está organizada solo por el nombre de la persona, la capacidad de procesamiento máxima del algoritmo es de 10 personas sin perjudicar el tiempo de ejecución, la base de datos y el procesamiento de maquina esta proporcionado por la placa de desarrollo que se utilice.

El sistema propuesto es confiable para la implementación en el hogar y otorgará seguridad y confort a la hora de instalarlo como control de acceso.

## 14. RECOMENDACIONES Y TRABAJOS FUTUROS

- El Desarrollo de este proyecto como se evidencio, busca la seguridad y confort en el hogar, por lo tanto, se espera que otros proyectos enfocados en los mismos ámbitos implementados en el hogar, puedan ser unificados con este proyecto, siendo así parte de un sistema más robusto y tecnológico, el cual tendrá muchas más funcionalidades que el actual proyecto, desde un control lumínico hasta el control de temperatura y todo controlado desde la placa de desarrollo Raspberry pi 3 B+.
- El sistema desarrollado en el presente trabajo puede llevarse a la industria, de tal forma que dote a varios sectores de la economía con un sistema de seguridad que identifique a las personas cuando ingresen a ciertos sectores restringidos, y este a su vez puede funcionar en conjunto con los sistemas ya instalados.
- Este proyecto puede ser usado para proponer mecanismos donde se utilice machine learning o aprendizaje de máquina y dotar al sistema de cierto conocimiento para detectar estados anímicos de la persona que ingreso a la vivienda, y con esta información se podría gestionar, predecir y controlar desde un buen estado de salud hasta la automatización del hogar para controlar los estados de ánimo.

## 15. BIBLIOGRAFÍA

- Alberto, and Jerónimo Ríos. 2017. "Reconocimiento Facial Por El Método De Eigenfaces." *Pistas Educativas* 127 (04): 66–81. <http://itcelaya.edu.mx/ojs/index.php/pistas>.
- A. Ryan et al., "Automated Facial Expression Recognition System," 43rd Annual 2009 International Carnahan Conference on Security Technology, Zurich, 2009, pp. 172-177. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5335546&isnumber=5335506>
- BADARÓ, Sebastián; IBÁÑEZ, Leonardo Javier; AGÜERO, Martín Jorge. *Sistemas expertos: fundamentos, metodologías y aplicaciones*. Ciencia y tecnología, 2013, no 13, p. 349-364.
- B. K. Gunturk, A. U. Batur, Y. Altunbasak, M. H. Hayes and R. M. Mersereau, "Eigenface-domain super-resolution for face recognition," in *IEEE Transactions on Image Processing*, vol. 12, no. 5, pp. 597-606, May 2003. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1203152&isnumber=27096>
- CNPV (Censo Nacional de Población y Vivienda). 2018. "Contexto". DANE. Pag 15
- CEREZO, E., Baldassarri, S., Cuartero, E., Serón, F., Montoro, G., Haya, P. A., & Alamán, X. (2007). Agentes virtuales 3D para el control de entornos inteligentes domóticos. In *XIII Congreso Internacional de Interacción Persona-Ordenador* (pp. 363-372).
- DANE. 20 de septiembre de 2019. DANE información para todos, fuente: <https://www.dane.gov.co/>
- DELAC, K., M. Grgic, and P. Liatsis. 2008. "Appearance-Based Statistical Methods for Face Recognition," no. June: 151–58. <https://doi.org/10.1109/elmar.2005.193665>.
- DÍAZ Mario, Maldonado Andrés Luengas, Balance de la seguridad de Bogotá No.53, Camara y comercio de Bogotá, pag 9, ISSN 2248-4906, Disponible en: <http://hdl.handle.net/11520/23187>
- GARCÍA, Alberto. *Inteligencia Artificial. Fundamentos, práctica y aplicaciones*. Rc Libros, 2012.
- HOSPITAL del trabajador. 2018. "Ergonomía: adaptando el trabajo a las personas". ["https://www.hospitaldeltrabajador.cl/ht/Comunidad/GuiaSalud/Salud/Paginas/Ergonomia.aspx"](https://www.hospitaldeltrabajador.cl/ht/Comunidad/GuiaSalud/Salud/Paginas/Ergonomia.aspx)

IZAURIETA, Fernando; SAAVEDRA, Carlos. Redes neuronales artificiales. Departamento de Física, Universidad de Concepción Chile, 2000.

JAIME Medina 18 de abril de 2012. ¿Sensor CCD o CMOS? ¿Qué significa todo esto?. Parentesis.com.  
[https://www.parentesis.com/tutoriales/Sensor\\_CCD\\_o\\_CMOS\\_Que\\_significa\\_todo\\_esto](https://www.parentesis.com/tutoriales/Sensor_CCD_o_CMOS_Que_significa_todo_esto)

KNVUL Sheikh. 1 de agosto de 2017. Quedarse con la cara. *INVESTIGACION CIENTIFICA*, 711(15476), 5-6. Disponible en:  
<https://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/el-multiverso-cuntico-711/quedarse-con-la-cara-15476>

LIGHTPATH.Tarjetas Para Desarrollo de hardware. [Consulta 9 de agosto, 2019], disponible en: <http://www.lightpath.io/tarjetas-de-desarrollo/>

LORA, D.; et al. Sistema de Seguridad Basado en una Plataforma Heterogénea Distribuida. Enseñanza y Aprendizaje de Ingeniería de Computadores, 5: 29-38 (2015). [<http://hdl.handle.net/10481/36567>]

MAYORGA Patarroyo Nicolás, 20 de mayo 2019 “Lo que le podría costar instalar sistemas de seguridad en su hogar” Columna La Republica, consultado el 16 de junio de 2019, disponible en: <https://www.larepublica.co/consumo/lo-que-le-podria-costar-instalar-sistemas-de-seguridad-en-su-hogar-2863423>

MENESES alvaro, vargas cristian; diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco José de caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar; universidad distrital francisco José de caldas facultad de ingeniería ingeniería electrónica, disponible en : <http://repository.udistrital.edu.co/bitstream/11349/3430/1/vargasgarciacristiangerman2016.pdf>

MD. Nasimuzzaman Chowdhury, Md. Shiblee Nooman, Srijon Sarker. Access Control of Door and Home Security by Raspberry Pi Through Internet. International Journal of Scientific & Engineering Research, Volume 4, Issue 11, November-2013 ISSN 2229-5518.

Modi, Mitul, and Fedrik Macwan. 2014. “Face Detection Approaches: A Survey.” International Journal of Innovative Research in Science, Engineering and Technology 3 (4): 11107–16. [www.ijirset.com](http://www.ijirset.com)

MOLLOCANA, A., & del Rosario, G. (2018). Sistema domótico de apoyo para personas con discapacidad motriz mediante tecnología móvil y reconocimiento de voz (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en



Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones).

MOLINA Lopez, F., Briand, D., & de Rooij, N. F. (2012). All additive inkjet printed humidity sensors on plastic substrate. *Sensors and Actuators B: Chemical*, 166–167, 212–222. <<https://www.sciencedirect.com/science/article/pii/S0925400512001748>>

MUHAMMAD Sharif, Farah Naz, Mussarat Yasmin, Muhammad Alyas Shahid and Amjad Rehman. Face Recognition: A Survey. Department of Computer Science, Comsats Institute of Information technology WahCantt MIS Department CBA Salman bin Abdulaziz University Alkharj KSA.

M. J. Barrera, N. Londoño, J. E. Carvajal and A. Fonseca, "Análisis y diseño de un prototipo de sistema domótico de bajo costo", *Rev. Fac. Ing. Univ. Antioquia*, no. 63, pp. 117-128, 2012.

PARDO Nicolás, 03 de octubre 2018 "La tecnología al beneficio de la seguridad ciudadana" *Columna el espectador*, consultado el 3 de junio de 2019, disponible en: <https://www.elespectador.com/opinion/la-tecnologia-al-beneficio-de-la-seguridad-ciudadana-columna-816004>

P. B. Balla and K. T. Jadhao, "IoT Based Facial Recognition Security System," 2018 International Conference on Smart City and Emerging Technology (ICSCET),

MUHAMMAD Sharif, Farah Naz, Mussarat Yasmin, Muhammad Alyas Shahid, and Amjad Rehman. 2017. "Face Recognition: A Survey" 10 (2): 166–77.

MUMBAI, 2018, pp. 1-4. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8537344&isnumber=8537238>

P. Kakumanu, S. Makrogiannis, N. Bourbakis. 2007. "A survey of skin-color modeling and detection methods" ITRI/Department of Computer Science and Engineering, Wright State University, Dayton OH 45435, USA. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.3484&rep=rep1&type=pdf>

PRESLER, Ari M. Digital camera system for recording, editing and visualizing images. U.S. Patent No 9, 565,419, 7 Feb. 2017

RESENDÍZ, G., Mendéz, E., Sanchez, A. L., & Gudiño, F. (2017). Integración de técnicas de inteligencia artificial en ambiente domótico. *Research in Computing Science*, 135, 85-98.

RUDY Lang, Michael Lescisin, and Qusay H. Mahmoud. June 2018. "Selecting a development board for your capstone or course project" 2-9.

SERACIS. Control de acceso. [Consulta 20 de mayo, 2019], disponible en <https://www.seracis.com/apoyos-detalle/controles-de-acceso>

SERRATOSA, F. (n.d.). La biometría para la identificación de las personas, disponible en: [https://www.academia.edu/31531606/La\\_biometria\\_para\\_la\\_identificacion\\_de\\_las\\_personas\\_Francesc\\_Serratosa\\_PID\\_00195448](https://www.academia.edu/31531606/La_biometria_para_la_identificacion_de_las_personas_Francesc_Serratosa_PID_00195448)

SIERRA, E., Hossian, A., García-Martínez, R., & Marino, P. (2005). Sistema experto para control inteligente de las variables ambientales de un edificio energéticamente eficiente. Proceedings de la XI Reunión de Trabajo en Procesamiento de la Información y Control. Universidad Nacional de Río Cuarto. Pág, 446-452.

SHINWARI, Ali Rehman. 2019. "A Comparative Study of Face Recognition under Pose Variation," 137–41.

TD sistemas control y gestión, Qué es un sistema de control de acceso [Consulta 20 de mayo, 2019], disponible en: <https://www.tdsistemas.com/que-es-un-sistema-de-control-de-acceso/>

VEGA Luna, J. I., Sánchez-Rangel, F. J., Salgado-Guzmán, G., & Lagos-Acosta, M. (2018). Sistema de acceso usando una tarjeta RFID y verificación de rostro. Ingenius, (20), 108-118. doi:<http://dx.doi.org.ucatolica.basesdedatosezproxy.com/10.17163/ings.n20.201>

Wainschenker, Rubén. 2011. "Procesamiento Digital de Imágenes Objetivos de La Materia."

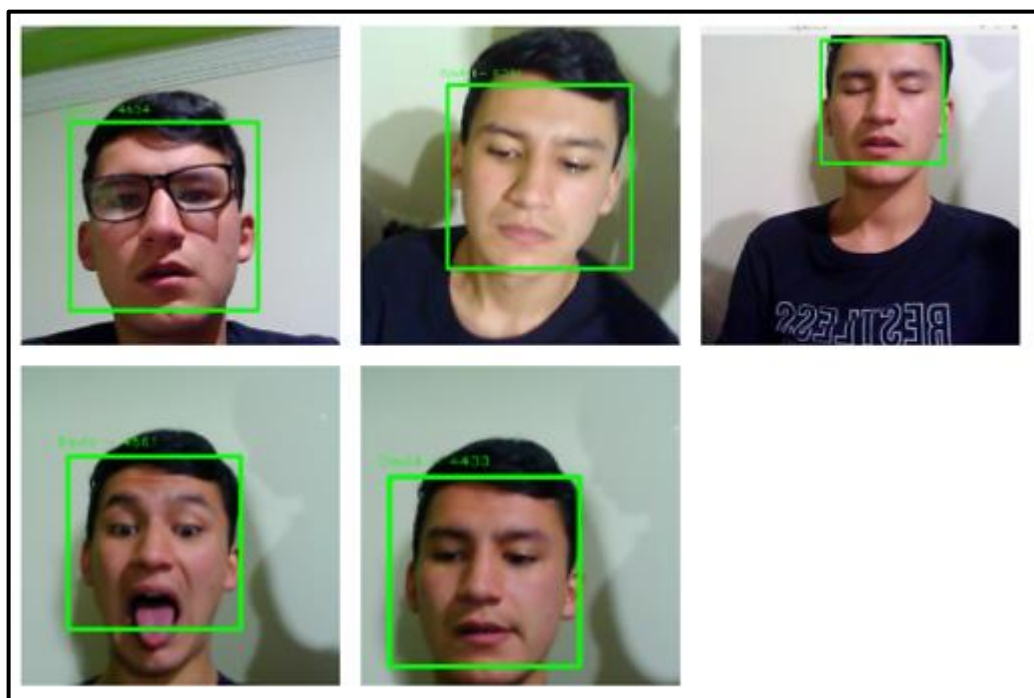
## ANEXOS

### ANEXO A

Este anexo contiene algunas de las fotos de test que se tomaron para verificar la eficiencia del sistema de reconocimiento facial, estas características son las más relevantes para la persona en cuestión.

En la figura 85, se evidencia fotos de test de David en la cual se puede ver pruebas con gafas, con gestos, también se puede evidencia que se toma la prueba desde un ángulo de 30°

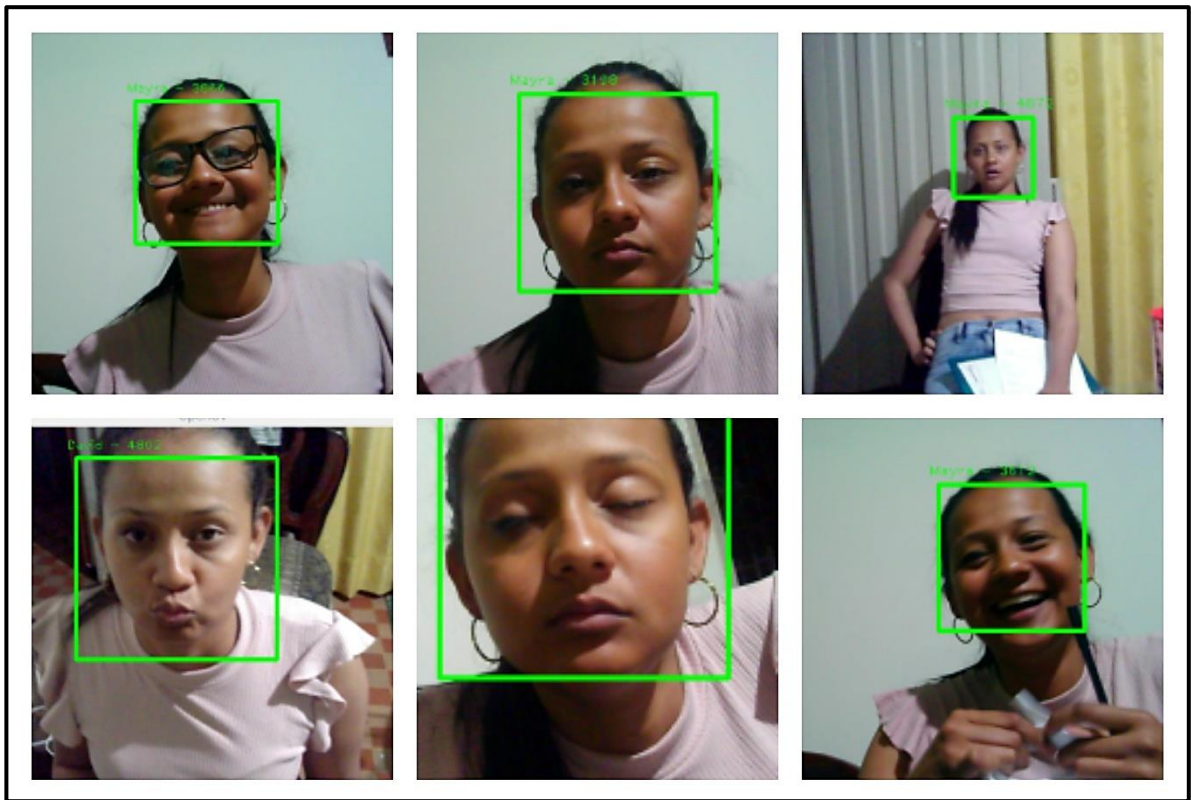
Figura 85. Pruebas David.



Fuente: Autores.

En la figura 86, se evidencia las pruebas de reconocimiento de Mayra donde se exponen las fotos con expresiones o gestos faciales, como la de sonrisa o de mueca, además, contiene la prueba de accesorios y un ángulo de 30°

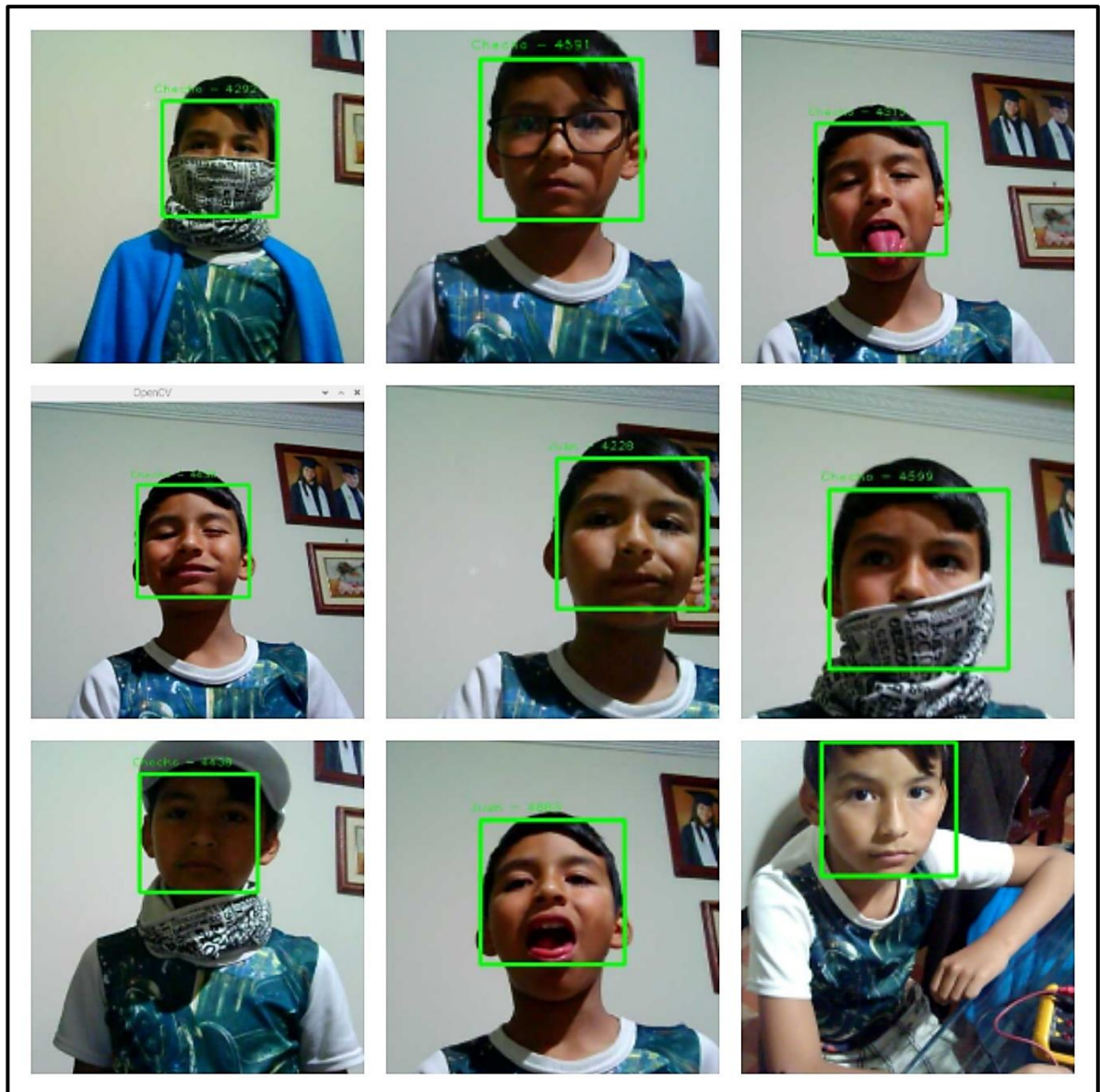
Figura 86. Pruebas Mayra.



Fuente: Autores.

En la figura 87, se ilustran las imágenes del test de Checho quien realiza pruebas con varias características y gestos faciales tales como muecas, y gestos que no se encontraban en el estudio y entrenamiento del algoritmo, además de esto se usa accesorios tales como una gorra, gafas, y hasta una bufanda, también se realizaron pruebas desde un ángulo de inclinación de 30°.

Figura 87. Pruebas Checho.



Fuente: Autores.

En la figura 88, se encuentran las imágenes de test de Juan quien realizó pruebas con algunos accesorios como gafas, gorras y una bufanda además de esto se adiciona pruebas con varios gestos y una prueba que se toma a una distancia considerable para medir la escala en la que el sistema puede reconocer



Figura 88. Pruebas Juan.



Fuente: Autores.

## ANEXO B

### Código de captura.

Figura 89. Código de captura parte 1.

```
1  import tkinter as tk
2  import cv2, sys, numpy, os
3  import numpy as np
4  from io import open
5  from tkinter import messagebox
6  from tkinter import ttk
7  from tkinter import *
8
9  def pulsar():
10     size = 4
11     fn_haar = 'haarcascade_frontalface_alt.xml'
12     fn_dir = '/home/pi/Desktop/ReconocimientoFacialTesis/caras'
13     ventana.destroy()
14     fn_name=nombre.get()
15     print(nombre.get())
16     path = os.path.join(fn_dir, fn_name)
17     if not os.path.isdir(path):
18         os.mkdir(path)
19     (im_width, im_height) = (112, 92)
20     haar_cascade = cv2.CascadeClassifier(fn_haar)
21     webcam = cv2.VideoCapture(0)
22     NumeroFotos =150
23     count = 0
24     while count < NumeroFotos:
25         (rval, im) = webcam.read()
26         im = cv2.flip(im, 1, 0)
27         gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
28         mini = cv2.resize(gray, (gray.shape[1] // size, gray.shape[0] // size))
29         faces = haar_cascade.detectMultiScale(mini)
30         faces = sorted(faces, key=lambda x: x[3])
31         if faces:
32             face_i = faces[0]
33             (x, y, w, h) = [v * size for v in face_i]
34             face = gray[y:y + h, x:x + w]
35             face_resize = cv2.resize(face, (im_width, im_height))
36             pin=sorted([int(n[:n.find('.')]) for n in os.listdir(path)
37                 if n[0]!='.' ]+[0])[-1] + 1
38             cv2.imwrite('%s/%s.png' % (path, pin), face_resize)
39             cv2.rectangle(im, (x, y), (x + w, y + h), (0, 255, 0), 3)
```

Fuente: Autores.

Figura 90. Código de captura parte 2.

```
40 ✓ cv2.putText(im, fn_name, (x - 10, y - 10), cv2.FONT_HERSHEY_PLAIN,
41 | 1,(0, 255, 0))
42 | count += 1
43 | cv2.imshow('OpenCV', im)
44 |
45 |
46 | key = cv2.waitKey(10)
47 ✓ | if key == 27:
48 | | break
49 |
50 | print('Fotografias finalizadas')
51 | (images, lables, names, id) = ([], [], {}, 0)
52 ✓ | for (subdirs, dirs, files) in os.walk(fn_dir):
53 ✓ | | for subdir in dirs:
54 | | | names[id] = subdir
55 | | | subjectpath = os.path.join(fn_dir, subdir)
56 ✓ | | | for filename in os.listdir(subjectpath):
57 | | | | path = subjectpath + '/' + filename
58 | | | | lable = id
59 | | | | images.append(cv2.imread(path, 0))
60 | | | | lables.append(int(lable))
61 | | | id += 1
62 | (im_width, im_height) = (112, 92)
63 | (images, lables) = [numpy.array(lis) for lis in [images, lables]]
64 |
65 ✓ | def validar():
66 ✓ | | if (cajatexto1.get()=="s" or cajatexto1.get()=="S"):
67 | | | ventana1.destroy()
68 | | | print(['Comenzando el entrenamiento'])
69 | | | model0 = cv2.face.createEigenFaceRecognizer()
70 | | | model0.train(images, lables)
71 | | | model0.save("Entrenador.yml")
72 | | | print('Entrenamiento completado con exito')
73 | | | messagebox.showwarning("Warning" ,"Entrenamiento finalizado")
74 | | | print('Programa finalizado')
75 ✓ | | else:
76 | | | ventana1.destroy()
77 | | | messagebox.showwarning("Warning" ,"Programa finalizado")
78 | | | print('Programa finalizado')
```

Fuente: Autores.



Figura 91. Código de captura parte 3.

```
78         print('Programa finalizado')
79
80     ventana1=Tk()
81     ventana1.geometry('220x90')
82     ventana1.title("Entrenador")
83
84     etiqueta1=Label(ventana1,text='¿Desea entrenar el modelo? S/N')
85     etiqueta1.place(x=1,y=1)
86
87     boton1=Button(ventana1,text='Ok', command=validar)
88     boton1.place(x=80,y=50)
89
90     nombre1=StringVar()
91     cajatexto1=Entry(ventana1,textvariable=nombre1)
92     cajatexto1.place(x=20,y=20)
93
94     ventana1.mainloop()
95
96     ventana=Tk()
97     ventana.geometry('300x100')
98     ventana.title("Registro")
99
100    etiqueta=Label(ventana,text='Nombre:')
101    etiqueta.place(x=20,y=20)
102
103    boton=Button(ventana,text='Registrar',command=pulsar)
104    boton.place(x=100,y=60)
105
106    nombre=StringVar()
107    cajatexto=Entry(ventana,textvariable=nombre)
108    cajatexto.place(x=100,y=20)
109
110    ventana.mainloop()
```

Fuente: Autores.

## ANEXO C

### Código de Reconocimiento

Figura 92. Código de reconocimiento parte 1.

```
1  import RPi.GPIO as GPIO
2  import time
3  import cv2, sys, numpy, os, time, webbrowser, signal
4  from cv2 import *
5  size = 4
6  fn_haar = 'haarcascade_frontalface_alt.xml'
7  fn_dir = '/home/pi/Desktop/ReconocimientoFacialTesis/caras'
8  os.system("clear")
9  (images, lables, names, id) = ([], [], {}, 0)
10 for (subdirs, dirs, files) in os.walk(fn_dir):
11     for subdir in dirs:
12         names[id] = subdir
13         subjectpath = os.path.join(fn_dir, subdir)
14         for filename in os.listdir(subjectpath):
15             path = subjectpath + '/' + filename
16             lable = id
17             images.append(cv2.imread(path, 0))
18             lables.append(int(lable))
19         id += 1
20 (im_width, im_height) = (112, 92)
21 (images, lables) = [numpy.array(lis) for lis in [images, lables]]
22 model1 = cv2.face.createEigenFaceRecognizer()
23 model1.load("Entrenador.yml")
24 cDavid = 0
25 cJuan = 0
26 cMayra = 0
27 cChecho = 0
28 cDaniel = 0
29 Seguridad = 10
30 webcam = cv2.VideoCapture(0)
31 while True:
32     (rval, frame) = webcam.read()
33     frame=cv2.flip(frame,1,0)
34     gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
35     mini = cv2.resize(gray, (gray.shape[1] // size, gray.shape[0] // size))
36     faces = cv2.CascadeClassifier(fn_haar).detectMultiScale(mini)
37     for i in range(len(faces)):
38         face_i = faces[i]
39         (x, y, w, h) = [v * size for v in face_i]
```

Fuente: Autores.

Figura 93. Código de reconocimiento parte 2.

```
40 face = gray[y:y + h, x:x + w]
41 face_resize = cv2.resize(face, (im_width, im_height))
42 print("reconociendo1")
43 prediction = model1.predict(face_resize)
44 cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0), 3)
45 print("reconociendo2")
46 print("reconociendo3")
47 if prediction[1]>500:
48     cv2.putText(frame, '%s - %.0f' % (names[prediction[0]],prediction[1]),(x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
49     cara = '%s' % (names[prediction[0]])
50     if cara == "David":
51         cv2.putText(frame,
52             'David',
53             (x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
54         cv2.imshow('OpenCV', frame)
55         cJuan = 0
56         cMayra = 0
57         cChecho = 0
58         cDaniel = 0
59         cDavid = cDavid + 1
60         if cDavid == Seguridad:
61             print('Se ha detectado a:')
62             print(cara)
63             url = "https://www.xbox.com/es-co"
64             webbrowser.open_new(url)
65             GPIO.setmode(GPIO.BOARD)
66             GPIO.setup(40, GPIO.OUT)
67             GPIO.output(40, True)
68             time.sleep(7)
69             GPIO.output(40, False)
70             print("Si desea analizar otra cara digite 1")
71             rep = int(input('En caso contrario digite 0\n'))
72             if rep == 0:
73                 os.kill(os.getppid(), signal.SIGHUP)
74             else:
75                 cDavid = 0
76                 os.system("clear")
77
```

Fuente: Autores.

Figura 94. Código de reconocimiento parte 3.

```
78  ✓ if cara == "Juan":
79      cv2.putText(frame,
80          'Juan',
81          (x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
82      cv2.imshow('OpenCV', frame)
83      cDavid = 0
84      cMayra = 0
85      cChecho = 0
86      cDaniel = 0
87      cJuan = cJuan + 1
88  ✓ if cJuan == Seguridad:
89      print('Se ha detectado a:')
90      print(cara)
91      url = "https://www.youtube.com"
92      webbrowser.open_new(url)
93      GPIO.setmode(GPIO.BOARD)
94      GPIO.setup(40, GPIO.OUT)
95      GPIO.output(40, True)
96      time.sleep(7)
97      GPIO.output(40, False)
98      print("Si desea analizar otra cara digite 1")
99      rep = int(input('En caso contrario digite 0\n')) )
100  ✓ if rep == 0:
101      |     os.kill(os.getppid(), signal.SIGHUP)
102  ✓ else:
103      |     cJuan = 0
104      |     os.system("clear")
105
106  ✓ if cara == "Mayra":
107      cv2.putText(frame,
108          'Mayra',
109          (x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
110      cv2.imshow('OpenCV', frame)
111      cDavid = 0
112      cJuan = 0
113      cChecho = 0
114      cDaniel = 0
115      cMayra = cMayra + 1
116  ✓ if cMayra == Seguridad:
```

Fuente: Autores.

Figura 95. Código de reconocimiento parte 4.

```
117     print('Se ha detectado a:')
118     print(cara)
119     url = "https://www.youtube.com/watch?v=8jwbnGrX7-c"
120     webbrowser.open_new(url)
121     GPIO.setmode(GPIO.BOARD)
122     GPIO.setup(40, GPIO.OUT)
123     GPIO.output(40, True)
124     time.sleep(7)
125     GPIO.output(40, False)
126     print("Si desea analizar otra cara digite 1")
127     rep = int(input('En caso contrario digite 0\n') )
128     if rep == 0:
129         os.kill(os.getppid(), signal.SIGHUP)
130     else:
131         cMayra = 0
132         os.system("clear")
133
134     if cara == "Checho":
135         cv2.putText(frame,
136             'Checho',
137             (x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
138         cv2.imshow('OpenCV', frame)
139         cDavid = 0
140         cJuan = 0
141         cMayra = 0
142         cDaniel = 0
143         cChecho = cChecho + 1
144         if cChecho == Seguridad:
145             print('Se ha detectado a:')
146             print(cara)
147             url = "https://www.youtube.com/watch?v=1RWqYR3e7xE&list=RD1RWqYR3e7xE&start_radio=1"
148             webbrowser.open_new(url)
149             GPIO.setmode(GPIO.BOARD)
150             GPIO.setup(40, GPIO.OUT)
151             GPIO.output(40, True)
152             time.sleep(7)
153             GPIO.output(40, False)
154             print("Si desea analizar otra cara digite 1")
155             rep = int(input('En caso contrario digite 0\n') )
```

Fuente: Autores.

Figura 96. Código de reconocimiento parte 5.

```
156         if rep == 0:
157             os.kill(os.getppid(), signal.SIGHUP)
158         else:
159             cChecho = 0
160             os.system("clear")
161
162     if cara == "Daniel":
163         cv2.putText(frame,
164             'Daniel',
165             (x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
166         cv2.imshow('OpenCV', frame)
167         cDavid = 0
168         cJuan = 0
169         cMayra = 0
170         cChecho = 0
171         cDaniel = cDaniel + 1
172         if cDaniel == Seguridad:
173             print('Se ha detectado a:')
174             print(cara)
175             url = "https://www.youtube.com/watch?v=1RWqYR3e7xE&list=RD1RWqYR3e7xE&start_radio=1"
176             webbrowser.open_new(url)
177             GPIO.setmode(GPIO.BOARD)
178             GPIO.setup(40, GPIO.OUT)
179             GPIO.output(40, True)
180             time.sleep(7)
181             GPIO.output(40, False)
182             print("Si desea analizar otra cara digite 1")
183             rep = int(input('En caso contrario digite 0\n') )
184             if rep == 0:
185                 os.kill(os.getppid(), signal.SIGHUP)
186             else:
187                 cDaniel = 0
188                 os.system("clear")
189
190     key = cv2.waitKey(10)
191     if key == 27:
192         break
```

Fuente: Autores.

## ANEXO D

### Código de la Interfaz.

Figura 97. Código de interfaz parte 1.

```
1  import RPi.GPIO as GPIO
2  import webbrowser as wb
3  import tkinter as tk
4  import os
5  import time
6  from io import open
7  from tkinter import messagebox
8  from tkinter import ttk
9  from tkinter import *
10 def admin():
11     def abrirventana2():
12         ventana.withdraw()
13         win=tk.Toplevel()
14         win.geometry('380x300+800+300')
15         win.configure(background="black")
16         win.title("Administrador")
17         def eliminar():
18             wb.open_new('/home/pi/Desktop/ReconocimientoFacialTesis/caras')
19         def captura():
20             os.system("python3 capture.py")
21             e3=tk.Label(win,text="Bienvenido a la Administración",bg="red",fg="white")
22             e3.pack(padx=5,pady=5,ipadx=5,ipady=5,fill=tk.X)
23             boton2=tk.Button(win,text="Registrar", bg="black",fg="white",command=captura)
24             boton2.pack(side=tk.TOP)
25             boton98=tk.Button(win,text="Modificar", bg="black",fg="white", command=eliminar)
26             boton98.place(x=5, y=42, width=130, height=30)
27             boton99=tk.Button(win,text="Eliminar",bg="black",fg="white",command=eliminar)
28             boton99.place(x=245, y=42, width=130, height=30)
29         def validar():
30             if entrada1.get()=="David" and entrada2.get()=="12345":
31                 abrirventana2()
32             elif entrada1.get()=="Juan" and entrada2.get()=="12345":
33                 abrirventana2()
34             else:
35                 messagebox.showwarning("Warning", "clave o usuario incorrectos")
36         ventana=tk.Toplevel()
37         ventana.title("Clave de administración")
38         ventana.geometry("380x300+800+300")
39         ventana.configure(background="black")
```

Fuente: Autores.

Figura 98. Código de interfaz parte 2.

```
40 e1=tk.Label(ventana,text="Username: ",bg="black",fg="white")
41 e1.pack(padx=5,pady=5,ipadx=5,ipady=5)
42 entrada1=tk.Entry(ventana)
43 entrada1.pack(fill=tk.X,padx=5,pady=5,ipadx=5,ipady=5)
44 e1=tk.Label(ventana,text="Password: ",bg="black",fg="white")
45 e1.pack(padx=5,pady=5,ipadx=5,ipady=5)
46 entrada2=tk.Entry(ventana)
47 entrada2.pack(fill=tk.X,padx=5,pady=5,ipadx=5,ipady=5)
48 boton3=tk.Button(ventana,text="Entrar",bg="black",fg="white",command=validar)
49 boton3.pack(side=tk.TOP)
50 def clave ():
51     def validar2():
52         if user1.get()=="David" and passd2.get()=="12345":
53             GPIO.setmode(GPIO.BOARD)
54             GPIO.setup(40, GPIO.OUT)
55             GPIO.output(40, True)
56             time.sleep(7)
57             GPIO.output(40, False)
58             messagebox.showwarning("Warning","Acceso correcto")
59         elif (user1.get()=="Juan" and passd2.get()=="12345"):
60             GPIO.setmode(GPIO.BOARD)
61             GPIO.setup(40, GPIO.OUT)
62             GPIO.output(40, True)
63             time.sleep(7)
64             GPIO.output(40, False)
65             messagebox.showwarning("Warning","Acceso correcto")
66         else:
67             messagebox.showwarning("Warning", "clave o usuario incorrectos")
68
69 ingreso=tk.Toplevel()
70 ingreso.title("Clave de ingreso")
71 ingreso.geometry("380x300+800+300")
72 ingreso.configure(background="black")
73 e6=tk.Label(ingreso,text="Username: ",bg="black",fg="white")
74 e6.pack(padx=5,pady=5,ipadx=5,ipady=5)
75
76 user1=tk.Entry(ingreso)
77 user1.pack(fill=tk.X,padx=5,pady=5,ipadx=5,ipady=5)
78 e1=tk.Label(ingreso,text="Password: ",bg="black",fg="white")
```

Fuente: Autores.



Figura 99. Código de interfaz parte 3.

```
79     e1.pack(padx=5,pady=5,ipadx=5,ipady=5)
80
81     passd2=tk.Entry(ingreso)
82     passd2.pack(fill=tk.X,padx=5,pady=5,ipadx=5,ipady=5)
83
84     boton8=tk.Button(ingreso,text="Validar password", bg="black",fg="white",command=validar2)
85     boton8.pack(side=tk.TOP)
86
87     pri =tk.Tk()
88     pri.geometry('2000x2000')
89     pri.configure(background= 'black')
90     pri.title("Reconocimiento facial")
91     e3=tk.Label(pri,text="Bienvenido",bg="black",fg="white")
92     e3.pack(padx=5,pady=5,ipadx=5,ipady=5,fill=tk.X)
93     imagen=PhotoImage(file="reco.png")
94     fondo=Label(pri,image=imagen).place(x=1,y=40)
95
96     def reconocimiento():
97         os.system("python3 reconocimiento.py")
98     e4=tk.Button(pri,text="Entrar por reconocimiento facial",bg="black",fg="white",command=reconocimiento)
99     e4.place(x=160, y=610, width=220, height=70)
100
101     boton7=tk.Button(pri,text="Entrar por clave usuario",bg="black",fg="white", command= clave)
102     boton7.place(x=160, y=530, width=220, height=70)
103
104     boton4=tk.Button(pri,text="Configuracion",bg="black",fg="white", command= admin)
105     boton4.place(x=160, y=450, width=220, height=70)
106     |
107     pri.mainloop()
```

Fuente: Autores.